PRIVACY IN PERSPECTIVE

Fred H. Cate

for the American Enterprise Institute

February 25, 2001

CONTENTS

EXECUTIVE SUMMARY iv

ABOUT THE AUTHOR vii

ACKNOWLEDGMENTS vii

INTRODUCTION 1

THE CURRENT PRIVACY DEBATE 2
1. Features of the Current Debate 3
2. The Range of Privacy Definitions 4
3. Consumer Concerns 4
4. Privacy as Control of Information 5
5. The Need for Specificity 6

THE VALUE OF INFORMATION AND THE BENEFITS THAT FLOW FROM ITS USE 7
1. The Information Infrastructure 8
   a. Expanding the Availability, Enhancing the Speed, and Lowering the Cost of Consumer Credit 8
   b. Identifying and Meeting Consumer Needs 9
   c. Enhancing Customer Convenience and Service 9
   d. Targeting Interested Consumers 10
   e. Promoting Competition and Innovation 10
   f. Preventing and Detecting Fraud 11
   g. Informing the Electorate and Protecting the Public 11
2. The Privacy Tension and the Limits of Consent 12
   a. Unanticipated Benefits 13
   b. Lack of Consumer Contact 13
   c. Value of Standardized and Third-Party Information 13
   d. Consumer Preferences 14
   e. The Practical Obstacles to Consumer Contact 14
   f. The Interconnectedness of Consent 14
   g. Required Consent 15
   h. Consumer Ignorance and Lethargy 15

THE ARSENAL OF PRIVACY TOOLS 16
1. Individual Judgment and Activity 16
2. Technologies 17
3. Self-Regulation 17
   a. Individual Institution Privacy Policies 17

b. Industry Association Standards and Services 18
c. Privacy-Specific Self-Regulatory Programs 18

THE ROLE OF LAW 19
1. Substantive Limits on Collection or Use 19
2. Enforcement of "Voluntary" Undertakings 20
3. Procedural Limits on Collection or Use 20
a. Notice 21
b. Choice 23
c. Access 26
d. Security 30
4. Other Issues 31
a. Enforcement 31
b. Preemption 32

THE COST OF PRIVACY LAWS AND REGULATIONS 33

THE CONSTITUTIONALITY OF PRIVACY LAWS AND REGULATIONS 35

THE IMPORTANCE OF CONTEXT 38

CONCLUSION: THE GOALS OF PRIVACY PROTECTION 40

NOTES 43

APPENDIX: Participants in the American Enterprise Institute's Privacy Roundtable 50

EXECUTIVE SUMMARY

As the 107th Congress convenes in Washington and state legislatures come into session around the country, the debate over "privacy" continues to escalate. Yet for all of its intensity there is a surprising lack of attention to the practical trade-offs inherently involved in restricting information flows in an effort to protect privacy.

To be certain, privacy is important and should be protected. But using law to protect privacy inevitably imposes costs—economic and otherwise—and those costs can be very significant, given the critical roles that information plays in our 21st century economy.

The Benefits of Accessible Information

For example, readily accessible, routinely collected information has greatly expanded the availability, increased the speed, and reduced the cost of consumer credit—by $80 billion a year for mortgages alone. Such information is also critical to identifying and meeting consumer needs, enhancing consumer convenience and service, and improving the accuracy and efficiency with which consumers can learn of products and services most likely to be of interest to them.

All of these benefits highlight the critical role of accessible information in treating customers as *individuals*, no matter how far away they may be located. Loan decisions can now be based on individuals' own record, not on local biases or prejudices. Financial services companies can aggregate customer deposits across accounts to waive fees or provide discounts. Businesses (or political campaigns, charitable groups, or alumni associations) can use personal information to target their offers based on consumers' demonstrated preferences.

Personal information is also a critical tool for promoting competition and innovation in the market. This is especially true on the Internet, where data constitute the only way that most customers and businesses ever know each other. Information is critical to fraud prevention and detection, apprehending criminals, tracking down missing persons and "deadbeat" parents, providing product safety recalls, and countless other valuable activities.

In sum, as the Federal Reserve Board has noted, information truly is the "cornerstone of a democratic society and market economy," constituting an essential, often invisible infrastructure

The Price of Privacy.

Efforts to craft legal protections for privacy inevitably interfere with this infrastructure and the benefits that flow from information-sharing. The absence of reliable information drives up costs, restrains competition, and restricts consumer convenience and service. More importantly, privacy laws can also harm the public welfare. For example, restrictive health privacy regulations adopted by states and, most recently, by the federal government, not only threaten to increase the

cost of health care while restricting its availability, but also have been demonstrated to interfere with medical research and the development of new treatments and drugs.

The Limits of Consent

Proponents of privacy laws argue that they merely wish to enhance consumer control over information about them. However, consent requirements often impose a considerable burden on consumers, in the form of increased contacts from institutions seeking consent, services delayed or denied because the of the difficulties of obtaining consent, and higher prices to cover the cost of seeking consent.

Moreover, conditioning the use of such information on consumer consent is often tantamount to prohibiting the use outright because of the cost of obtaining consent, the extent to which selectivity in the information included undermines its usefulness, the degree to which uses of information are interconnected, and the many impediments to consumers receiving and acting on the request for consent, even when it is in their best interest to do so. Because the opportunity to consent can also interfere with the prevention and detection of fraud and other crimes, compromise the quality of health care, and otherwise block broad, socially valuable uses of information, this "individualist vision threatens the entire community."

Before adopting privacy laws, therefore, legislators need to recognize the extent to which both information flows benefit consumers, businesses, and the entire economy, and privacy laws interfere with those benefits.

The Role of the Government

Of course, not all legislative efforts to protect privacy need be regulatory in nature. Legislators play other critical roles in helping to protect individual privacy. One of the most important responsibilities of the government is assuring that its own house is in order. Only the government has the power to compel disclosure of personal information and only the government operates free from market competition and consumer preferences. As a result, the government has special obligations to ensure that it complies with the laws applicable to it; collects no more information than necessary from and about its citizens; employs consistent, prominent information policies through public agencies; and protects against unauthorized access to citizens' personal information by government employees and contractors.

Similarly, there are many steps that only the government can take to protect citizens against privacy-related harms, such as identity theft: Make government-issued forms for identification harder to obtain; make the promise of centralized reporting of identity thefts a reality; make it easier to correct judicial and criminal records and to remove permanently from one individual's record references to acts committed by an identity thief. The government alone has this power.

Regulators and law enforcement officials should enforce existing privacy laws vigorously, and legislators should ensure that they have the resources to do so.

The government should also help educate the public about privacy and the tools available to every citizen to protect her own privacy. Many privacy protections can only be used by individuals—no one else can protect their privacy for them. Yet few individuals will recognize the importance of their responsibility or have the knowledge to fulfill it without education.

The Challenge for Lawmakers

When new laws or regulations are thought necessary, it is critical to identify and articulate clearly the purpose of the proposed privacy law or regulation, and whether it will in fact serve that purpose: In sum, what public benefit justifies the government's action? Only after having answered this question can the benefits of the proposed law or regulation be balanced against both the beneficial uses of information with which it interferes and the other costs of implementing and complying with the law. Armed with this information, lawmakers must then ask whether the law is worth its cost or whether there are other less intrusive, less expensive, or more effective tools for achieving the same purpose.

Finally, lawmakers must determine that the law is constitutionally permissible—a considerable hurdle in light of the fact that when privacy and First Amendment expression rights conflict, the Supreme Court has consistently found that the latter prevail. In answering all of these questions, consumers, businesses, and rational lawmaking all benefit from a close and careful scrutiny of the specific requirements of the proposed law or regulation and the specific contexts in which it will operate.

About the Author

Fred H. Cate is a Visiting Scholar at the American Enterprise Institute; Professor of Law and Harry T. Ice Faculty Fellow at the Indiana University School of Law—Bloomington; and Senior Counsel for Information Law with Ice Miller Legal & Business Advisors.

He appears regularly before Congress, state legislatures, and professional and industry groups on privacy and other information law issues. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities, served as vice chair of the American Bar Association Section on Health Law's Electronic Communications and Privacy Interest Group, and was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security.

Professor Cate is the author of many articles and books concerning privacy and information law, including the award-winning *Privacy in the Information Age* and *The Internet and the First Amendment*. He is the co-author of the sixth edition of *Mass Media Law* (with Marc Franklin and David Anderson). He received his J.D. and his A.B. with Honors and Distinction from Stanford University.

Acknowledgments

The author thanks the participants in the American Enterprise Institute's privacy roundtable and especially Professor Paul Schwartz for his detailed comments and careful editing; Peter Wallison of the American Enterprise Institute, for the opportunity to prepare this paper and for his wise insight; and Jean Walker and Melissa Luftig for their excellent research assistance.

INTRODUCTION

The debate over "privacy" continues to escalate in Washington and other national and state capitals. Yet for all of its intensity there is a surprising lack of attention to the practical ramifications of protecting, or failing to protect, privacy. Participants in the privacy debate employ catchphrases like "opt-in" and "opt-out" with little regard for what they signify. Widely divergent types of information are lumped together without regard for the sensitivity or risks associated with them. The debate often ignores the economic and technical realities that shape how information is used and how it may be protected. Even on the most basic concepts—such as the meaning of "privacy" or the goal of laws intended to protect it—the debate lacks not only consensus, but even clarity or specificity on the points of disagreement.

The words of Commissioner Orson Swindle, dissenting from the Federal Trade Commission's (FTC) recommendation for online privacy regulation, apply with equal force to much of the current privacy debate:

> [It] fails to pose and answer the most basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced.[1]

To be certain, privacy is important and should be guarded. But using law to protect privacy inevitably imposes costs—economic and otherwise—and those costs can be very significant given the critical roles that information plays in our 21st century economy. The challenge lawmakers face is to recognize those trade-offs and to balance privacy protection with its inevitable costs. This is not an easy task. Given the extraordinary practical and constitutional significance of both information flows and privacy, the potential cost of inadequate or inappropriate privacy regulation is significant.

To help address this problem, the American Enterprise Institute is publishing *Privacy in Perspective*. The purpose of the document is reflected in its title: to add perspective to the privacy debate. The pages that follow seek to outline the complexity of the issues and stakes in the privacy debate, put that debate in a practical context, define key concepts and policy alternatives, and identify the likely ramifications of each. This document does not advocate a particular outcome, but rather seeks to help inform the privacy debate and provide it with greater structure and rationality.

Privacy in Perspective grew out of a unique program in which the American Enterprise Institute invited a dozen privacy experts to spend a day together in an off-the-record roundtable about the ramifications of laws and regulations designed to protect privacy. The group could hardly have been more diverse: It included attorneys and economists; academics and practitioners;

recognized authorities on technology, journalism, and consumer affairs; members of the private, public, and not-for-profit sectors; and, most important, a wide range of perspectives on the role of the government with regard to privacy and information flows. (A list of participants is attached.)

The group met without a formal agenda or an audience. There were no prepared papers or presentations. Instead, the participants identified a wide range of interests and issues that are affected by privacy laws and regulations, and the trade-offs that lawmakers face whenever they act to protect privacy.

Privacy in Perspective expands on that discussion. The author and the American Enterprise Institute gratefully acknowledge the generously shared expertise and insight of the participants. While this document reflects the input of many (and each participant had an opportunity to review a draft of the text prior to publication), it does not purport to represent any consensus or the views of any institution or individual other than the author. Rather, it reflects one effort to provide legislators and others with basic information about how personal information is used in the economy and the trade-offs inherent in restricting those uses to protect privacy.

THE CURRENT PRIVACY DEBATE

The past two years have witnessed an avalanche of privacy activity, including comprehensive federal financial privacy legislation enacted as part of the Gramm-Leach-Bliley Financial Services Modernization Act (Gramm-Leach-Bliley),[2] the first federal law prohibiting access to historically open public records without individual "opt-in" consent,[3] sweeping health privacy rules adopted under the Health Insurance Portability and Accountability Act (HIPAA),[4] children's online privacy rules promulgated by the FTC,[5] multimillion dollar settlements of privacy lawsuits, a multistate attorneys general privacy investigation of major banks,[6] the negotiation of a privacy "safe harbor" with European regulators, the appointment of the first ever federal privacy official, two proposals from the FTC for legislation concerning online privacy,[7] two Supreme Court cases upholding privacy laws from constitutional attack,[8] and more than 600 privacy bills proposed in Congress and state legislatures.

Congress has formed a bipartisan, bicameral Congressional Privacy Caucus, and a number of privacy bills are already pending.[9] The FTC is expanding its online profiling inquiry to include offline profiling.[10] The National Association of Attorneys General (NAAG) in December released a draft statement on Privacy Principles and Background calling on Congress to enact broad new privacy laws.[11] States are implementing the Gramm-Leach-Bliley provisions applicable to insurance companies, and are already considering many bills on public records privacy, identity theft, telemarketing, and other issues. In short, the privacy debate is at a fevered pitch and federal and state legislators are being called on to evaluate an array of proposals for more legislation. The starting place for that assessment is recognizing the unique features of the privacy debate, the many meanings of "privacy," the variety of concerns that prompt privacy laws, and the variety of objectives that privacy laws may serve.

1. Features of the Current Debate

The political debate over privacy and the role of the government in protecting it is unusual because of a confluence of factors:

- Privacy is important for all individuals in a wide variety of settings. Because it involves restrictions on the information flows that are essential to consumer products and services, commerce, and government, the debate over how to protect privacy affects all citizens, consumers, most businesses, government agencies, and other institutions.

- The benefits that result from open information flows (and that are therefore put at risk when privacy protections interfere with those flows) are so integral a part of our lives that they are seldom explicitly recognized or fully understood.

- By contrast, almost everyone believes they understand privacy and know how at least their privacy should be protected.

- Privacy is a subjective and often emotional issue: What threatens one individual's sense of privacy may not concern another person.

- Most people regard privacy, or at least their own privacy, as deserving of as much protection as possible: If a little is good, more is even better.

- The rhetoric of the privacy debate runs the risk of distorting its outcome. As Kent Walker has written: "Just as no one is 'pro-abortion' or 'anti-life,' no one can be 'anti-privacy,' yet that's the only label left by the rhetoric."[12]

- The polling data on privacy is highly contradictory, perhaps reflecting the wide variety of meanings given the term "privacy" (see below). For example, in one 1999 poll published in the *Wall Street Journal*, 29% of people surveyed listed loss of privacy as the issue that concerns them most about the 21st century—ahead of terrorism on U.S. soil, world war, global warming, or economic depression.[13] Yet a 2000 survey of registered voters in five states selected because of the high degree of attention paid to privacy in their legislatures and press—California, New York, Massachusetts, Texas, and Washington—found that only 1% of respondents mentioned "privacy" as "one of the most important issues or problems that State legislatures should address."[14]

Collectively, these factors have contributed to diminishing the rationality of the current privacy debate, while escalating the pressure on legislators to "do something" to protect privacy.

2. The Range of Privacy Definitions

In addition, the many recent and pending privacy enactments reflect a wide variety of understandings for what "privacy" means, including:

- individual autonomy (the right to make decisions about marriage or family without government interference);

- solitude and intimacy (the desire to limit access to a place or to oneself);

- confidentiality (trade secrets and information disclosed subject to a promise of confidentiality);

- anonymity (the desire not to be identified);

- security (for oneself or one's information);

- freedom from intrusion (whether physical—a trespasser, or technological—a hidden camera or microphone); and

- control of information about oneself.

Historically, some of these concepts of privacy (such as the right to make decisions about marriage or family, or to be free from government intrusion) are protected by law, and often constitutional law. Other concepts (such as solitude and intimacy) are not directly protected by law, but rather by strong social norms.

3. Consumer Concerns

Concerns about privacy touch on a wide variety of issues. Among the most prominent in the current debate are fears about:

- surreptitious collection of personal information (such as undisclosed monitoring of browsing habits);

- reuse of personal information for purposes other than those for which it was collected;

- combining or matching personal information collected from disparate sources (profiling);

- transfer (or, more accurately, the replication) of personal information to third parties (whether through sale, rental, or exchange, and including the use of personal information by one company to market the products or services of another company);

- interception or misappropriation of personal information (whether by third-party "hacking" or the unauthorized acts of employees or contractors);

- use of personal information to commit fraud or cause physical or emotional harm (fraudulent charges on credit cards, identity theft, stalking);

- intrusive or annoying use of personal information (telemarketing);

- maintenance and use of inaccurate personal information (thereby denying the consumer benefits to which he or she is otherwise entitled or marketing products or services in which a consumer is unlikely to be interested); and

- indefinite retention of personal information (so that the consumer is hard-pressed to move beyond past mistakes).

The current privacy debate also reflects a number of tangential issues, for example, concerns about the proliferation of information technologies, the imbalance of bargaining power between individuals and institutions, the desire of individuals to define for themselves the image they present to the world, the forces of globalization, aggressive marketing tactics, computer viruses, and a general sense of loss of control.

4. Privacy as Control of Information

Historically, U.S. privacy regulation has focused on preventing uses of information that *harm* consumers, such as for credit card fraud. Under this approach to privacy, the law does not regulate information flows generally or grant to consumers the legal right to control nonharmful uses of personal information. This approach therefore avoids both interfering with the availability of information for socially or economically valuable uses and running afoul of the First Amendment, which the Supreme Court has interpreted as allowing any use of information that does not cause a specific harm. (Both the benefits of information flows and the constitutional protection for those flows are discussed in greater detail below.[15])

One variation on the understanding of privacy as the right to be free from harmful uses of information is an approach that permits any use of information is acceptable as long as it is *compatible* with the reason for which the information was first provided. Sometimes referred to as "implied consent," this approach recognizes that many uses of information are so consistent with the reasons for which the consumer first provided the information or are so clearly in the best interest of the consumer, that consent should be implied. However, some uses may be so incompatible that the law allows consumers to block them. For example, under the Fair Credit Reporting Act (FCRA), credit-related information may be collected and used without consumer consent only for the "permissible purposes" set forth in the statute.[16] The European Union's data protection directive dispenses with the requirement for consent when a proposed use of information is necessary to complete a transaction initiated by the consumer.[17]

Increasingly, however, the dominant trend in recent and pending privacy legislation is to invest consumers with near absolute *control over information*, what Alan Westin, in his path-breaking study *Privacy and Freedom*, described as "the claim of individuals, groups, or

institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[18] Public officials and privacy advocates argue that "we must assure consumers that they have full *control* over their personal information"[19] and that privacy is "an issue that will not go away until every single American has the right to *control* how their personal information is or isn't used."[20] NAAG's December 2000 draft statement on Privacy Principles and Background sets forth as its core principle: "Put simply, consumers should have the right to know and *control* what data is being collected about them and how it is being used, whether it is offline or online."[21] And virtually all of the privacy bills pending before Congress reflect this goal: "To strengthen *control* by consumers" and "to provide greater individual *control*."[22]

Recent legislation, therefore, is not limited to allowing consumers to block harmful or incompatible uses of information about them, but instead increasingly conditions the collection, transfer, and any whatever of personal information, no matter how innocuous or beneficial, on consumer consent. In fact, some privacy advocates have gone so far as to argue that individuals have a *property* right in information about them, so that any use of that information without consent would constitute trespass. This approach ignores the practical difficulty and burden to consumers of attempting to exercise control over the vast amount of data that they generate and disclose about themselves in a increasingly networked economy, conflicts with Supreme Court precedent,[23] violates the First Amendment,[24] and ignores the many powerful reasons why society requires access to information about others.[25] But it does suggest how far toward the understanding of privacy as *control* the current debate has moved.

5. The Need for Specificity

It is critical for legislators to identify the privacy interest a proposed law is intended to serve, so that they can determine whether a need exists, whether the law in fact meets that need, and whether there are less expensive or burdensome ways of accomplishing the same end. Much of the current privacy debate lacks that specificity. For example, in an effort to address one of consumers' most commonly cited privacy concerns—telemarketing—legislatures have considered (and in some cases adopted) a wide range of laws establishing "do-not-call" lists and prohibiting the use of certain types of personal information in telemarketing solicitations. Laws establishing "do-not-call" lists reflect an effort to protect *solitude* or guard against *intrusion* into the home. Laws prohibiting the use of personal information (such as data about past purchases) when telemarketing respond to concerns about *control* of information, but would do nothing for concerns about intrusion into the solitude of the home. In fact, by making it harder to target telemarketing calls to specific individuals, such laws actually *increase* calls into the home, because businesses would have to place *more* calls to reach the same number of people who would likely be interested in their products or services.

Greater precision regarding the purpose of privacy protections may also help reduce or better focus some of the emotional sensitivity in the current privacy debate. As we have seen, the term "privacy" is used to refer to a wide variety of interests and concerns. As a result, we use the same term—"privacy"—to describe fundamental interests—such as being free from government

searches of homes and persons, and from government interference with decisions about religion, voting, health care, marriage, procreation, child rearing, and education—as well as more mundane or technical issues about the type and frequency of notice about information-sharing that must be provided by a financial institution to consumers or by a health care provider to patients. Upon rational reflection, it is likely that most people would regard these interests as being of a wholly different magnitude and therefore warranting a different type of legal response.

Because the current privacy debate uses one term to describe such widely divergent interests, and that term provokes such an emotional response because of the significance of *some* of the interests to which it is applied, it has become increasingly difficult to assess thoughtfully which privacy interests warrant legal protection and how much cost for that protection is justified. Like the boy who cried "wolf," we run the risk of diluting our social and legal commitment to protecting fundamental privacy interests if we approach all privacy issues with the same fervor and regulatory zeal. Greater specificity in identifying the privacy interest at stake, the harm a proposed law will address, whether the law is likely to be effective in preventing or remedying that harm, and whether the cost of that law is justified in relation to the harm will help focus our resources and our outrage on the privacy issues that warrant them.

THE VALUE OF INFORMATION AND THE BENEFITS THAT FLOW FROM ITS USE

People need privacy. Privacy is critical to citizen participation in this society and democracy and to consumer participation in commerce, especially online; privacy protection is therefore key to the growth and success of commerce online and off. If individuals fear that their information is inadequately protected and may be used to harm them they may refuse to participate altogether, or they may withhold or distort relevant information, thereby denying others access to accurate information and wasting resources. For example, a patient who fears that the results of a genetic screening test may be used to harm her may avoid having the test and therefore delay treatment or counseling.

However, privacy does not exist in a vacuum: It is always in tension with other important values and with the benefits that result from open information flows. Consumers' desire for greater privacy is always in tension with their desire for other benefits, such as convenience and low cost, with which privacy protection often interferes. Lawmakers face a considerable challenge when trying to craft privacy protections without diminishing the benefits of open information flows.

To fully understand this point it is necessary to recognize, first, the extent to which the benefits, services, and convenience that consumers expect depend on the availability of reliable, standardized personal information, and, second, the extent to which privacy protections hinder access to that personal information.

1. The Information Infrastructure

Information is the lifeblood of our 21st century economy. In the words of the Federal Reserve Board: "[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."[26] These simple words reflect a profound transformation: Consumers are increasingly evaluated today according to more complete, objective, and reliable information about them than was ever before possible. As a result, consumers can now expect—and the law can meaningfully require—that they be judged on their own records, not by their race, gender, who they know, or other subjective prejudices. This is the result of the information revolution: Routine, comprehensive information collection has contributed to unprecedented prosperity, and allows more Americans than ever before to share in that prosperity, and to do so on a more equitable basis. Consider the following examples of benefits that this "information infrastructure" makes possible.

a. Expanding the Availability, Enhancing the Speed, and Lowering the Cost of Consumer Credit

The routine sharing of reliable, standardized personal information has greatly expanded the availability, increased the speed, and reduced the cost of consumer credit. So, for example, when a consumer applies for a mortgage, car loan, or instant credit, the lender makes its decisions about whether, how much, and on what terms to lend based on information collected from a wide variety of sources over time. The lender can have confidence in that information because it has been assembled routinely—not just for the purpose of one loan application—and presents a complete picture of the borrower's financial situation—not just one moment in time or information from just a selective sample of the businesses with which the borrower deals. Because of that confidence, lenders provide more loans to a wider range of people than ever before. Between 1956 and 1998, the number of U.S. households with mortgage loans more than trebled. The same trend is true for credit card products; today, the average American adult carries 13 credit cards.

Consumers benefit by obtaining the funds they need to buy homes and cars and finance educations. The "almost universal reporting" of personal credit histories, in the words of economist Walter Kitchenman (a participant in the American Enterprise Institute's privacy roundtable), is the "foundation" of consumer credit in the United States and a "secret ingredient of the U.S. economy's resilience."[27] In addition, because the necessary information does not have to be collected from scratch, loan applications are reviewed and approved faster than ever before. In 1997, 82% of automobile loan applicants received a decision within an hour; 48% of applicants received a decision within 30 minutes.[28] Many retailers open new charge accounts for customers at the point of sale in less than two minutes. This is unheard of in countries where restrictive laws prevent credit bureaus and other businesses from routinely collecting the information on consumer activities required to maintain the accurate, up-to-date files necessary to support rapid and accurate decision making.

The greater accuracy, speed, and efficiency of the credit system, and the greater confidence of lenders also drives down the cost of credit. Lenders don't have to charge higher

interest rates and fees to guard against bad or missing information. And it is easier for lenders to pool loans according to risk and sell them in the secondary market—a process known as "securitization." This makes more capital available for new loans and further reduces the cost of credit in the United States by an estimated $80 *billion* per year for mortgages alone.[29] Most importantly, consumers benefit from the knowledge that loan decisions will now be based on their own financial situation, not on local biases or prejudices. Readily available, standardized personal information not only makes this possible, it also facilitates easy analysis of lender compliance with fair lending laws.

b. Identifying and Meeting Consumer Needs

Businesses use personal information to identify and meet customer needs. According to Federal Reserve Board Governor Edward Gramlich: "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences."[30] In short, information-sharing allows businesses to ascertain customer needs accurately and meet those needs rapidly and efficiently. Detailed consumer information is at the heart of new individualized offerings that provide each customer with the recognition and personalized service that she desires.

c. Enhancing Customer Convenience and Service

Information-sharing also enhances customer convenience and service. For example, many services are provided through a myriad of companies. A customer may have a checking account, a savings account, a credit card, and an investment account all with the same bank, but the four services will likely be provided by four completely separate affiliates. The customer's checks will be printed by a separate company altogether. Billing for the credit card may be handled by still another company. Because of information-sharing, the customer can deal with all six entities as if they were one. Her high savings balance may be used to qualify her for free checking. Overdrafts on her checking account can be covered automatically with her credit card. She can call one customer service number with questions, and if her credit card or checks are stolen, a single call is all that is needed to protect all of her accounts.

Many retailers provide specialty services and products, such as fine jewelry, photographic studios, vision services, hair care, and product repair or installation through independent companies that license the retailer's name, but are not the retailer's affiliates. This approach is required because of the nature of the service, efficiencies that come with specialization, insurance factors, and federal and state tax and licensure laws. Due to routine information-sharing, these independent companies provide services to customers under the retailer's name, accept the retailer's credit card, include information and coupons in the retailer's mailings and advertisements, participate in the retailer's loyalty programs, and, from a customer perspective, are simply another department of the retailer's operations.

d. Targeting Interested Consumers

Information-sharing also allows consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested. As a result, information on second mortgages and home improvement services can be targeted only to home owners. Information on automotive products and services are targeted only to car owners. The American Association of Retired People can target its offers only to older Americans, veteran's organizations can appeal only to people who have served in the armed forces, and political campaigns can target their solicitations to registered members of their party.

In the absence of information-sharing, these organizations either (1) could not afford to communicate with potential customers or members, or (2) they must contact even more households—meaning more unsolicited mail, e-mail, and telephone calls—to find people interested in their offer. The first alternative would mean the death of many organizations. In fact, the cost of alerting consumers about a new product or opportunity can be a major obstacle to the launch of new businesses and prevent innovative products from ever reaching the marketplace. The second alternative means that the public is peppered with more mail, e-mail, and telephone calls, a higher percentage of which will be of no interest to the recipient. This would truly be "junk mail," because it would have been generated without regard for the recipient's demonstrated interests. Targeting marketing to consumer interests lowers the volume, cost, and environmental impact of that marketing while increasing consumer satisfaction.

e. Promoting Competition and Innovation

Information-sharing is especially critical for new and smaller businesses, which lack extensive customer lists of their own or the resources to engage in mass marketing to reach consumers likely to be interested in their products or services. This may help explain why some large European national banks and industrial concerns supported new privacy laws there: By restricting the availability of information about their customers, privacy laws help to protect established businesses from competition from other countries or start-ups. Open access to third-party information and the responsible use of that information for targeted marketing is essential to level the playing field for new market entrants.

Similarly, businesses offering specialized products and services rely on accessible information to help them identify and reach those customers most likely to be interested in their offerings, wherever those customers are located. Many businesses in today's markets never see their customers because transactions are conducted exclusively by telephone, Internet, or mail. These businesses are able to serve the needs of potential customers they have never met because of the free flowing information that allows them to identify who those likely customers are. In a global market, information-sharing is key to connecting far-flung customers and businesses.

f. Preventing and Detecting Fraud

Another key use of personal information is to prevent and detect fraud. More than 1.2 million worthless checks are cashed at retailers, banks, and other U.S. businesses every day, accounting for more than $12 billion in annual losses.[31] Treasury Department officials estimated that credit card fraud losses would be between $2 billion and $3 billion in 2000.[32] The insurance industry paid $24 billion—10% of all claims—in 1999 for fraudulent property and casualty claims.[33] The GAO found that Medicare made improper payments of $13.5 billion in fiscal year 1999 alone, and has estimated that health care fraud accounts for up to 10% of national health care spending each year.[34] Across the economy, business losses due to all forms of document fraud and counterfeiting exceed $400 billion—6% of annual revenue of American businesses—per year.[35] Although businesses paid for virtually all of these losses, they ultimately affect consumers through higher prices, inconvenience, and lost time and productivity.

Personal information is one of the most effective tools for stemming these losses. Such information is used every day to identify consumers cashing checks and seeking access to accounts. Close monitoring of account activity also allows credit providers, insurance companies, and other businesses to recognize unusual behavior that may indicate that someone is using a credit card or debit card without authorization or making improper claims. Moreover, because of information-sharing, companies share alerts about lost or stolen credit or debit cards and information about fraud schemes so that they can prevent further losses and improve the odds of apprehending the thief.

g. Informing the Electorate and Protecting the Public

Personal information is also used for a wide variety of purposes central to democratic self-governance and protecting public health and safety. For example, information is used to elect and monitor public officials and to facilitate public oversight of government employees and contractors. The Supreme Court has found that these uses are so critical that it has eliminated any recourse by public officials or public figures for the publication of true information, even if defamatory or highly personal.[36]

Law enforcement officials rely on collected personal information to prevent, detect, and solve crimes. Journalists and other researchers use accessible information to inform the public about matters of public importance. Personal information is also used for product safety warnings and recall notices, such as when Firestone and Ford Motor Company used databases to identify and obtain current addresses for people who own recalled Firestone tires.

Medical researchers rely heavily on personal information to conduct "chart reviews" and perform other research that is critical to evaluating medical treatments, detecting harmful drug interactions, uncovering dangerous side effects of medical treatments and products, and developing new therapies. Such research *cannot* be undertaken with wholly anonymous information, because the detailed data that researchers require will always include information that *could* be used to identify a specific person, and when that information indicates that a given therapy or drug poses a real health risk, researchers *must* notify the affected individuals.

Even information as mundane as citizen addresses is used to locate missing family members, owners of lost or stolen property, organ and tissue donors, and members of associations and religious groups and graduates of schools and colleges; and to identify and locate suspects, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. (This same information is used to help verify the identity of consumers who apply for instant credit, begin new utility service, or seek other valuable products and services.)

These examples are not exhaustive; they are mere illustrations of the extent to which personal information constitutes part of this nation's essential infrastructure, the benefits of which are so numerous and diverse that they impact virtually every facet of American life.

2. The Privacy Tension and the Limits of Consent

All of the benefits outlined above flow from readily accessible information about consumers. To provide those and other benefits, access to data is essential. Laws and regulations designed to protect privacy interfere with that access and therefore with the benefits that result from open information flows. In the words of one state Attorney General, because privacy laws interfere with information flows, consumers ultimately pay the price for those laws "in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace."[37]

Proponents of new privacy laws often argue that businesses and other organizations merely need to educate consumers about the benefits of information flows, and then those individuals will consent to the collection and use of information about them. The simple, straightforward nature of this argument has made it very powerful, but it is often wrong, for at least eight reasons: (1) consumers are often unwilling to consent to the use of information because the benefits that flow from that use are unanticipated; (2) the companies that use personal information in ways that benefit consumers may have no direct contact with those consumers; (3) the real value of the information may be that it is collected routinely and without consumer consent; (4) consumers expect that information will be used to determine their eligibility for valuable offers and are often annoyed at being asked to consent to such uses; (5) it is often difficult or even impossible to reach consumers to obtain their consent; (6) because so many beneficial uses of information are interconnected, some uses of information are only possible and affordable because the information is also used for other purposes; (7) consent may be irrelevant because the service or product cannot be provided without the use of information; and (8) few consumers take the time to review offers to determine whether they wish to consent, so that consent may not be obtained no matter how desirable or beneficial the proposed use of information. Each of these is discussed in greater detail below.

a. Unanticipated Benefits

The benefits of personal information are often unanticipated. For example, many retailers collect information about consumer purchases and then access that information so that consumers can return merchandise without a receipt, order supplies and replacement parts without knowing the exact model number or specific product information, obtain information about past purchases for insurance claims when fire or other disasters destroy or damage those goods, and receive immediate notification about product recalls and other safety issues. These are tangible benefits that many consumers take advantage of every day, but few consumers would anticipate in advance that they were going to need information about a past transaction for insurance purposes or to order replacement parts. The benefit is exceptionally valuable when it is needed, but often illusory before that time.

b. Lack of Consumer Contact

Many benefits result from uses of personal information that do not involve the consumer directly. For example, credit bureaus update consumer credit files—the files that are used to obtain rapid, low cost access to credit of all forms—without ever dealing directly with the consumer. In fact, few Americans will ever deal directly with a credit bureau. To require the credit bureau to establish contact with the consumer every time it needed to collect or use information about him or her would be expensive and burdensome to the consumer. Similarly, most mailing lists are obtained from third parties, not the people whose names are on the list. For a secondary user to have to contact every person individually to obtain consent to use the information would cause delay, require additional contacts with consumers, and increase costs.

c. Value of Standardized and Third-Party Information

There are many beneficial uses of personal information where the benefit, frankly, is derived from the fact that the consumer has *not* had control over the information. This is certainly true of credit information: Much of its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make not only that credit report useless, but all others, because lenders, merchants, employers, and others who rely on credit reports would not know which ones contained only selective information. Even when information is not particularly "positive" or "negative," its value may depend on it being complete. Many businesses monitor accounts for suspicious activity that may indicate fraudulent activity. Often credit card companies will call a card holder whose account has experienced unusual charges to verify that the card has not been stolen. Identifying the *unusual* requires knowing what is *usual* and that, in turn, requires access to a complete set of data.

d. Consumer Preferences

Most consumers do not want to be deluged with repeated requests for consent. The ultimate result is that consumers will either not consent, and thereby diminish the benefits that flow from information-sharing both for themselves and others, or they will consent to everything,

just to avoid further calls, letters, and e-mails. The *Los Angeles Times* reported in December 1999 that banking customers are understandably "irritated if the bank fails to inform them that they could save money by switching to a different type of checking account." As the newspaper noted, however, "to reach such a conclusion, the bank must analyze the customer's transactions."[38] One major U.S. bank reported that its customers who participated in a test of various privacy policies were annoyed at the very idea of being contacted by the bank to obtain permission to contact them again in the future to offer selected opportunities. Customers expected that the bank would use their information to offer them appropriate offers. The last thing they wanted was another phone call or letter asking permission to do what they perceived to be the very foundation of their relationship with the institution.

e. The Practical Obstacles to Consumer Contact

Conditioning use of personal information on specific consent may also harm consumers because of the practical difficulties of reaching many consumers. Consider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system ("opt-in" and "opt-out" are discussed in greater detail below[39]). To obtain permission to utilize information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls, and one-third of their customers were denied opportunities to receive information about valuable new products and services.[40]

f. The Interconnectedness of Consent

Many of the beneficial uses of information that consumers now enjoy depend on spreading the cost of collecting and maintaining the information for a variety of uses. For example, commercial intermediaries collect, organize, and make accessible to the public government records. Those records are used for countless socially valuable purposes: monitoring government operations, locating missing children, preventing and detecting crime, apprehending wanted criminals, securing payments from "deadbeat" parents and spouses, and many others. In fact, in 1998 the FBI alone made more than 53,000 inquiries to commercial online databases for "public record information" that led to the arrest of 393 fugitives wanted by the FBI, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.[41] The Association for Children for Enforcement of Support uses information from public records, provided through commercial vendors, to locate over 75% of the parents they sought.[42] Access to these records is possible, as well as convenient and inexpensive, precisely because commercial intermediaries assemble the information for such a wide variety of other uses. If the law restricted the other valuable uses of public records, or made those uses prohibitively expensive, then the data and systems to access them would not be in place for *any* use. In as much as the beneficial uses of information outlined above are interconnected, and often depend on common systems and

spreading the cost of acquiring and managing data over many uses, consent-based laws may only create the *illusion* of consent, because they will lead to consumers having fewer opportunities made available to them to which they *can* consent.

g. Required Consent

The opportunity for consent may also be illusory because many services or products cannot or will not be provided without personal information. HIPAA, for example, requires that physicians provide extensive disclosures and obtain explicit consent concerning information collection and use prior to treating a patient. If a patient wishes to be treated, he or she must consent. The law is effectively irrelevant, because the physician cannot treat the patient without information about his or her condition. Moreover, as a practical matter, signing the consent form is likely to become just another procedural hurdle, like signing an insurance authorization form, to getting in to see a doctor. Experience suggests that few people will shop for physicians based on information policies; rather, their decisions about from whom to seek service will be driven by price, location, insurance coverage, specialty, and other considerations. So the expense of crafting, providing, and storing consent forms will likely achieve little in terms of enhancing consumer choice or privacy.

h. Consumer Ignorance and Lethargy

Finally, even if the request gets through to the intended adult recipient, the typical response to requests for consent to use personal information, to judge by the extensive experience of businesses and not-for-profit organizations, is that the customers will simply ignore the request. Most unsolicited mail in this country is discarded without ever being read and most unsolicited commercial or fund-raising telephone calls are terminated by the consumer without the offer ever being made. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on. Even where mail is actually read and the offer appeals to the consumer, lethargy and the competing demands of busy lives usually conspire to ensure that no action is taken. It is difficult to imagine that promises of potential future benefits from information use will command greater attention or activity.

These considerations suggest that simply conditioning the use of personal information on specific consent is tantamount to prohibiting outright many beneficial uses of information, because of the cost of obtaining consent, the extent to which consent may undermine information's usefulness, the degree to which uses of information are interconnected, and the many impediments to consumers receiving and acting on the request, even when it is in their best interest to do so. Lawmakers should therefore scrutinize consent requirements carefully to ensure that they are not more intrusive than necessary to protect consumers from identified harms, and that they are worth the cost that they inevitably impose on consumers and businesses by restricting the benefits that result from information flows.

THE ARSENAL OF PRIVACY TOOLS

There are many tools for protecting privacy. Law is one of these tools, as is discussed in greater detail below,[43] but there are other important tools that warrant close consideration.

1. Individual Judgment and Activity

Among the wide variety of tools available to protect privacy, many of the most effective do not involve government invention. Perhaps the most basic privacy protection is personal judgment—being sensitive to privacy issues, determining when and to whom to reveal personal information, and taking steps to protect one's own privacy, such as protecting sensitive information. Although this type of individual action may have little impact on innocuous, routine information collection, it has the potential for limiting many harmful uses of information.

Individual action may provide the best defense to identify theft, for example. Despite all of the bills that have been introduced to combat identity theft, many of the most effective means continue to be those that individuals take to protect themselves: keeping a close watch on account activity; reporting suspicious or unfamiliar transactions promptly; properly destroying commercial solicitations; storing valuable documents securely; protecting account names and passwords; and never disclosing personal information to unknown callers. Moreover, legislation to prevent identity has proved problematic because of both significant under-enforcement and the fact that while legislation focuses on protecting against identity theft by strangers,[44] many—perhaps most—identity theft cases involve friends and family members of the victims.[45] The practical, specific steps that individuals can take protect them from both strangers and others, and do not depend on government enforcement.

Individual knowledge and action are also critical to take advantage of existing privacy protection tools (discussed in greater detail below[46]), such as credit bureau, individual company, and Direct Marketing Association services to remove them from mailing lists and prescreened offer lists; consumer rights under the Telephone Consumer Protection Act to avoid unwanted commercial telephone solicitations;[47] and "opt-out" rights under the FCRA[48] and Title V of Gramm-Leach-Bliley.[49] Participants in the privacy debate disagree about whether any of these alone is sufficient to protect privacy, but individual knowledge and action are certainly necessary.

This focus on individual action is especially important because no technology, self-regulatory scheme, or even law can substitute for good judgment in the management of personal information and identification documents, nor will any of these be effective if individuals do not know how to use them to protect their own privacy.

2. Technologies

One of the most effective steps that individuals can take to protect their privacy online is to employ widely available and easy-to-use technologies. Privacy settings in Internet browsers such as Netscape Navigator and Microsoft Explorer, stand-alone programs such as encryption

and firewall software, anonymization services, anonymous remailers, and other technologies offer individual users a high degree of customized control over their own personal information. And there are emerging initiatives, such as P3P, that promise an even higher degree of tailored privacy protection online.

Technologies are no panacea. They are very effective, however, in protecting against the surreptitious collection of the vast amounts of data generated by Web browsing—one of the most sensitive issues in the current privacy debate. Moreover, technologies, unlike law, also protect consumers from off-shore and fly-by-night actors.

3. Self-Regulation

"Self-regulation" may be subject to as many meanings as "privacy" itself. These may be divided generally into three broad categories.

a. Individual Institution Privacy Policies

The past decade has witnessed an extraordinary growth in the number of companies and other institutions that have adopted privacy policies. These provide consumers with varying degrees of notice about how these entities collect and use information about them and what options consumers have for controlling that collection and use. The FTC reported in May 2000 that the number of commercial Web sites with privacy policies had increased from 14% in 1998 to 88% in 2000. One hundred percent of the busiest commercial Web sites posted a privacy policy in 2000.[50] By contrast, this past summer the General Accounting Office found that only 85% of federal government agency Web sites posted a privacy policy[51] despite a directive more than a year earlier from Office of Management and Budget Director Jack Lew to do so.[52] A September 2000 Brown University study of 1,700 state and local government Web sites found that only 7% posted a privacy policy.[53]

Many companies actively compete for customers by promoting their privacy policies and practices. If enough consumers demand better privacy protection and back up that demand, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much society really values privacy.

b. Industry Association Standards and Services

Industry organizations are increasingly adopting standards for privacy protection and helping consumers whose privacy interests are compromised. The Direct Marketing Association (DMA), for example, operates the Mail, Telephone, and E-Mail Preference Services. With a single request to each, an individual can remove herself from DMA-member company mailing, telephone, and e-mail solicitation lists.[54] Corporate compliance with privacy standards constitutes an increasingly important accolade in competitive markets, particularly among Internet users.

Moreover, industry associations can help persuade member organizations to adopt and adhere to industry norms for privacy protection. The DMA, for example, has begun issuing quarterly reports on members who are being disciplined for violating DMA codes of conduct.

Privacy-specific industry organizations are also emerging. For example, the majority of companies providing look-up services on individuals has agreed to abide by the Individual Reference Services Group (IRSG) Principles, which not only establish data protection standards, but also require annual compliance audits by third parties and a commitment not to provide information to entities whose practices are inconsistent with the IRSG Principles.[55] Similarly, the major providers of online advertising formed a coalition, the Network Advertising Initiative, that promulgated a privacy code and provides a convenient way for consumers to "opt-out" of having personal information used to target banner advertising to them.[56]

The development and enforcement of industry standards contributes not only to enhancing privacy protection, but also to providing an easy way for consumers to distinguish between businesses that comply with those standards and businesses that do not. As industry standards become more pervasive, they have the effect of isolating and focusing scrutiny on noncomplying businesses.

c. Privacy-Specific Self-Regulatory Programs

Third-party self-regulatory organizations are also emerging to make privacy self-help easier on the Internet. TRUSTe is a program that rates Internet sites according to how well they protect individual privacy. Internet sites that provide sufficient protection for individual privacy—including not collecting personal information, not disseminating information to third parties, and not using information for secondary purposes without consent—earn the right to display the TRUSTe logo.[57] The Better Business Bureau has launched a similar initiative—BBB Online.[58]

Self-regulatory tools are often more flexible and more sensitive to specific contexts—and therefore allow individuals to determine a more tailored balance between information uses and privacy—than privacy laws. For example, government do-not-call lists and legal consent requirements usually present consumers with only a binary choice: all or nothing. Self-regulatory tools typically allow consumers to specify with far greater precision how they wish to be contacted and by whom. Moreover, self-regulatory tools can be changed more quickly in response to markets or technological developments. They are often less expensive to create and implement. They are exactly the type of responses we would expect to result from private sector markets if consumers value privacy protection.

Self-regulatory tools have been criticized as allowing too much flexibility, for example, when companies unilaterally alter their privacy policies. Because of the context-sensitivity of most self-regulatory tools, there is little standardization of their terms or how they operate, thereby requiring more attention from consumers who desire to take advantage of the privacy protections

they offer. Finally, self-regulatory tools require some form of investigatory and enforcement mechanisms so that consumers can have confidence that organizations are doing what they have pledged to, and have recourse in the event that they are not. The role of law as an integral component of effective self-regulation is discussed in greater detail below.[59]

THE ROLE OF LAW

Law also plays an important role in protecting privacy. The specific nature of that role varies widely depending upon the nature of the information, the context in which it is being collected or used, and, most significantly, whether the collection or use is by the government or a private party. In the context of private sector information processing, on which this document focuses, many laws regulate, directly or indirectly, information collection and use. These laws may be divided generally into three categories: laws that impose *substantive* restrictions on the collection and/or use of information; laws that provide for enforcement of privacy policies, contracts, and other *voluntary* undertakings; and laws that create *procedural* requirements governing the collection and use personal information.

1. Substantive Limits on Collection or Use

The first category includes laws that impose substantive limits on the collection and use of information. Such laws often are usually designed to serve some objective other than privacy. For example, the Equal Employment Opportunity Act prohibits discrimination in hiring, firing, or the terms of employment on the basis of an individual's "race, color, religion, sex, or national origin," but does not prohibit the collection, storage, or dissemination of such information.[60] Similarly, the Fair Housing Act prohibits discrimination in the sale or lease of housing on the basis of "race, color, religion, sex, familial status, or national origin," but is silent on all aspects of data processing.[61]

To the extent the legislative debate is focused on privacy as *control*, there are few laws that impose substantive limits on the collection or use of information, because the very objective of such substantive limits is to substitute the government's view for that of the individual either collecting or using the information. On the other hand, many of these laws protect against *harmful uses* of information. There is a wealth of state and federal privacy laws that prohibit such harmful uses as the fraudulent use of personal information, check and credit card fraud, identity theft, and impersonating another person.

2. Enforcement of "Voluntary" Undertakings

A second role that law plays in protecting privacy is holding information collectors and users and self-regulatory organizations to their voluntary undertakings. As we have seen, many businesses and other organizations provide privacy policies that set forth the organization's commitment regarding the collection and use of information. Even when the law requires these policies, their substantive content is largely determined by market pressures, consumer demands,

and management preferences. No matter the source of those undertakings, actions by the FTC, state attorneys general, and private litigants have demonstrated that they are conditions of the transaction by which information is provided and so may be enforced under federal and state consumer protection law and state contract law. In the online environment, for example, the FTC has brought and settled many cases in which it alleged that a Web site operator's failure to adhere to its privacy policy constituted an "unfair or deceptive" trade practice in violation of the Federal Trade Commission Act.[62] The law thus provides both an enforcement mechanism—the courts along with federal and state law enforcement officials—and a legal remedy for a voluntary undertaking.

3. Procedural Limits on Collection or Use

The third role that laws play in protecting privacy is to specify what may be thought of as *procedural* privacy protections. Rather than set specific substantive limits on information collection and use, these laws require that individuals be given notice of when information is to be collected, and that those individuals' wishes regarding information collection and use be respected. The current policy debate has focused on four "procedural" requirements: notice, choice, access, and security. These four requirements are the core of the FTC's proposal for online privacy legislation, the December 2000 NAAG privacy statement, the Congressional Privacy Caucus' privacy principles, and virtually all of the privacy bills currently pending before Congress.

Collectively, these four requirements are designed to serve the concept of privacy as *control*. Individuals must be informed prior to the collection or use of information about them. They must be given a choice as to whether to permit that collection or use. They must be given access to information about them so that they can both verify that no information has been collected without consent and have the opportunity to dispute or correct the accuracy of information. Finally, individuals must be assured that adequate security measures protect information about them so that no one else can obtain or use that information without their consent.

Within the current policy debate, a variety of often controversial issues have surrounded each of these four requirements. The resolution of those issues is critical to ensuring that privacy laws respond to real harms, prevent or remedy those harms as effectively as possible, and impose no greater cost than is necessary. Because of their prominence in the current privacy debate, those issues are addressed in detail below.

a. Notice

Virtually all recent and proposed privacy laws obligate collectors and users of information from or about consumers to provide consumers with "clear and conspicuous" notice of their information practices, including what information they collect; how they collect it; how they use it; how they provide choice, access, and security to consumers; and whether they disclose the

information collected to other entities.[63] Such a requirement raises many issues that lawmakers need to consider:

- What triggers the notice requirement—*collection* or *use* of information? Legislators should consider carefully the ramifications of requiring that notice be provided to a consumer in situations in which information is not being collected directly *from* that consumer (for example, when information is *observed* or is obtained from a third-party). This issue is complicated by requirements, such as those contained in Gramm-Leach-Bliley, that notice be provided annually, even if no new information has been collected or used.[64]

- How is notice to be provided? Increasingly, U.S. laws and regulations, like the privacy provisions of Gramm-Leach-Bliley and the privacy regulations promulgated under HIPAA,[65] are requiring that *individualized* notice be provided—that a notice be given or mailed to every consumer. The benefits of such a requirement must be balanced against its costs—measured not only in monetary terms, but also by the burden to consumers and businesses, and the delay in providing requested services. Legislators should also consider whether there are less expensive and burdensome alternative means for ensuring that consumers have meaningful notice of data processing practices—such as prominently posting or displaying a notice, as most Web sites do, or providing individual notification only that a notice exists, but providing the full text of the notice only upon request.

- When must notice be provided? Most proposals would require that notice be provided *before* any information is collected or used. Such a requirement is arguably necessary to give consumers a meaningful opportunity to decide whether to provide the information. It is not always possible, however, to provide notice before collecting or using information. This is especially true online, where personal information is required by the technologies that operate the Web in order to provide the pages that contain the notices. Similarly, if notices are to be mailed, addresses will have to be collected first.

- How should notices be written and what should they contain? Most recent privacy enactments and pending bills have used the phrase "clear and conspicuous" to describe both the placement and the terms of privacy notices, but this phrase has not quelled a growing debate over the detail required. Some have argued that notices should be warnings, like health warnings on cigarettes, that merely alert the consumer that information is being collected or used. Others, however, have argued that notices should be viewed as contracts and, thus, should both contain all of the material terms necessary to make those contracts complete, and be evaluated under strict liability. As the FTC and state attorneys general increasingly litigate the precision with which a business must adhere to its privacy notices, businesses are understandably making those notices more detailed and more qualified. Recent experience has shown that notices that are comprehensive are criticized as overly complex, but that notices that are succinct are criticized as incomplete and inaccurate. And legal liability can result from providing either

too much or too little specificity. The issue involves more than just compliance with applicable laws, but rather raises the question of who will really take the time to read and understand privacy notices.

- How can a notice be changed and with what effect? As technologies, markets, and financial conditions change, privacy notices are likely to require alteration over time. How are organizations to notify consumers of changes and what effect should changes have on data already collected? Network advertiser DoubleClick faced this issue when it acquired database company Abacus and wished to alter its policy on matching online and offline data. More than a dozen government and private lawsuits were filed as a result of DoubleClick's stated intention to change its policy, and the company's stock plummeted as a result of the controversy.[66] Toysmart raised this issue in the context of a bankruptcy proceeding in which the defunct toy retailer wished to sell its customer lists to satisfy creditors, despite a privacy policy prohibiting the sharing of such information. Amazon.com was strongly criticized when it notified each of its customers that it was altering its privacy policy. In each of these instances, efforts to change notices resulted in intense criticism, market disfavor, and/or litigation.

- Are there situations in which notice is inappropriate or even harmful? For example, should notice be required if the consumer has no choice about how information about him or her is used, if the only information being collected is publicly available, if the information reveals no sensitive or potentially harmful fact about an individual, or if notice is very expensive to provide? Historically, notice has not been universally required. For example, the FCRA imposes important limits on the use of consumer reports, but requires notice in very limited circumstances and only of a few specific information uses.[67] This reflects the policy decision that the value of the information routinely assembled is so great (even to consumers who at the time of its collection might not consent), the cost of providing notice and requiring consent at each point of collection and use so high, and the privacy risk associated with that information's collection and responsible use so low, that notice and consent should not be required. More recent legislation has not been as sensitive to the cost and value of providing notice. Gramm-Leach-Bliley requires notice even when there is no use of information to which the consumer may legally object.[68] NAAG has proposed requiring notice (and an opportunity to withhold consent) even when the information being collected is not personally identifiable.[69] The HIPAA regulations require detailed, formal notice even when the collection of information is apparent and no other use of the information is intended (for example, notice is required by a pharmacist before filling a prescription and from a physician before treating a patient).[70] Some would argue that, for other than highly sensitive personal information, if it is clear that personal information is being collected directly from a consumer, and the information is used for no purpose other than that for which the information is provided, formal or individualized notice should not be required. This reflects the fact that the "notice" principle is often referred to as the "knowledge" principle. Under this view, the issue is not notice, but rather whether the consumer has, or should have, *knowledge* about the data collection.

Where it is clear that the consumer does have that knowledge or that the requested service or product cannot be provided without the information, additional notice is meaningless.

b. Choice

Choice is an equally broad principle. Virtually all recent and proposed privacy laws require that personal information be collected or used only with consumer consent.[71] Choice is directly related to notice, because the consumer can only consent to that of which she is given notice. The scope of choice is therefore limited by the notice. An often unstated but clear corollary of choice is that no collection or use of information is allowed that is inconsistent with the consumer's choice.

The debate over choice generally focuses on two concepts: "opt-in" and "opt-out." Although these concepts are seldom defined in any detail, they reflect the nature of the choice given to the consumer. Under "opt-in," the consumer is asked to affirmatively express his consent to information collection or use. In the absence of the consumer's express permission, no information may be collected or used. Under "opt-out," the consumer is asked to indicate his objection to the information collection or use that he wishes to prevent. In the absence of the consumer's express opposition, information may be collected and used consistent with the notice provided to the consumer. Although at first blush these simplistic-sounding options may appear to be merely the opposite sides of the same coin, the reality is far more complex. Both options have raised many issues and together they provide the focal point of the current privacy debate.

Privacy advocates argue that "opt-out" is equivalent to data collection and use without consent because of the difficulty of finding and understanding many privacy notices, the lack of consumer knowledge or motivation necessary to object to proposed information gathering or use, and the inconvenience or difficulty of having to object to protect one's own privacy. Moreover, the "opt-out" system provides little legal incentive to businesses and other information users to make notices clearer or "opt-out" mechanisms more convenient because, in the absence of effective action by the consumer, the business is free to collect and use information. In an "opt-in" world, by contrast, privacy advocates argue that businesses and other information users would have every incentive to make notices clear and conspicuous and "opt-in" mechanisms easy to use, because in the absence of effective consumer action, the business could make no use of consumer information.

Free-flow advocates counter that "opt-out" and "opt-in" mechanisms both give consumers the final say about whether their information is collected and used. Neither approach gives individuals greater or lesser rights than the other. They argue, however, that shifting from an "opt-out" system to an "opt-in" system—while not increasing privacy protection—imposes significantly higher costs on consumers, businesses, and the economy as a whole, because of the difficulty of contacting consumers one-by-one to obtain their affirmative consent, as opposed to posting a notice to all consumers and letting consumers take advantage of 800-numbers and 24-hour customer service centers to express their objection to particular information uses. Moreover,

free-flow advocates argue, "opt-out" is more consistent with consumers' interests, since businesses make literally millions of uses of consumer data every day in an effort to meet customer needs, lower prices, and attract new customers: Most consumers do not want to be bothered by requests for consent to beneficial uses of largely innocuous data, and businesses have every incentive to tailor their data use to customer interests and preferences. This is why, many businesses argue, so few consumers take advantage of existing "opt-out" opportunities—not because they are unaware of them or don't know how to use them, but rather because they are happy with the information use and are satisfied in the knowledge that they *could* object if they wished to.[72]

Increasingly, while the "opt-out" and "opt-in" labels are bandied about in the privacy debate, the terms may not be that meaningful. In Europe, for example, where the law specifies "opt-in," many countries are using a concept of "implied opt-in"—implying "opt-in" consent from an individual's failure to object to a proposed use of information—which is difficult to distinguish from "opt-out." Whatever label is applied, choice raises a number of important issues, many of which were discussed above. In addition, lawmakers should consider:

- To what does "opt-out" or "opt-in" apply? Does it apply to information that explicitly identifies a person; information that could be used to identify a person; any information about or supplied by a person, even if it does not necessarily identify him or her; "sensitive" information; or even publicly available information? Similarly, to what uses of information does it apply—any collection or use of information, use of information only for marketing, or use of information only for some other specified purpose? Should the law require consent before using one's own information, information of an affiliate or subsidiary, or only if the information is obtained from a third party? The answers to these questions will dramatically affect the cost and burden on both consumers and businesses of providing choice.

- What does "opt-out" or "opt-in" require? For example, does "opt-in" mean no *collection* of information without consent, no *use* of information without consent, or no *matching* of information without consent? If "opt-in" extends to use of consumer information, how can a business request consent without using information for which consent is required?

- How broad or specific can consent be? Should the law set limits on the breadth of proposed use for which consent may be sought? Should consumers be asked to give or withhold consent to a single transaction (e.g., cashing a check), a type of transaction (e.g., all future check-cashing), a type of use of information defined by the data subject (e.g., for financial services only), or a type of use of information defined by its relationship to the purpose for which the information was originally provided or collected (e.g., cashing the check, collecting payment on it, and related activities only)? Can "opt-out" or "opt-in" be obtained for *all* future uses of information? Can either or both be extended to "compatible uses"?

- How is consent recorded? Must it be in writing or witnessed? Is oral consent ever appropriate?

- Can consent be withdrawn? If so, how, and with what effect on existing uses of the information?

- How will "opt-out" or "opt-in" work in practice? How easy must an "opt-out" opportunity be? Must it be free to the data subject? How will a business request "opt-in" consent if the information is being obtained from the data subject, if the information is being obtained from a third party, or if the information is being observed? How will consent for future uses, not contemplated at the time of the original consent, be sought? Recall that U.S. West found that it required an average of 4.8 calls to each customer household before it reached an adult who could grant consent, and that the company never reached one-third of its customers. How can the burden of "opt-in" or "opt-out" be reduced?

- What are the consequences of not providing consent? FTC Commissioner Robert Pitofsky, when he was Chairman, argued that in the online environment, service providers should not be able to condition service on consumers agreeing to uses of their information that are not required to provide the requested service.[73] The HIPAA health privacy rules prohibit health providers and payers from conditioning service on an individual's consent to uses of information that are not necessary to provide the service.[74] If the additional use of the information generates value (or reduces costs) for the service provider, should it be free to recognize that fact by doing business only with information-sharing customers or by offering those customers a discount or preferential service?

- Are there exceptions where businesses may use information without consent, such as emergencies (e.g., providing health records if data subject is unconscious), uses that benefit the data subject (e.g., warning of drug interactions), socially beneficial uses (e.g., fraud prevention and detection), or to contact the data subject to seek consent for some proposed use? May a business freely collect information that is not sensitive or that is observed in public without consumer notice or consent? May a business use information without consent to determine eligibility for an offer, or must it approach the individual once to seek permission to use her information to determine if she is eligible, and then a second time to tell her whether she qualified for the offer?

- Is there a constitutional difference between "opt-out" and "opt-in"? Constitutional issues generally are discussed below,[75] but a recent decision by the U.S. Court of Appeals for the Tenth Circuit, which the Supreme Court declined to review, suggests that there may be constitutional significance to the decision whether to require "opt-out" or "opt-in." The court, 2-1, struck down the rules of the Federal Communications Commission requiring that telephone companies obtain "opt-in" consent from their customers before using data about their customers' calling patterns to market products or services to them. The court

wrote that the government must show that the use of the information that the law would protect as private would inflict *"specific and significant harm*" on individuals and that "opt-out" consent would not be sufficient to prevent or remedy that harm.[76] The Tenth Circuit's decision reflects earlier U.S. Supreme Court decisions striking down "opt-in" requirements in other settings. The Supreme Court has struck has down ordinances that would require affirmative consent before receiving door-to-door solicitations,77 before receiving Communist literature,[78] even before receiving "patently offensive" cable programming.[79] The words of the Court in the 1943 case of *Martin v. Struthers*—involving a local ordinance that banned door-to-door solicitations without explicit ("opt-in") householder consent—are particularly apt: "Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community. In the instant case, the City of Struthers, Ohio, has attempted to make this decision for all its inhabitants."[80]

- Does *choice* mean more than *consent*? Although in the current privacy debate "choice" is used primarily to refer to whether a consumer consents to the collection and use of personal information and the method by which that consent is sought, it may actually be a much broader principle. Free-flow advocates argue that choice includes the consumer's right to make his or her own choice about the proper balance between the value of the open flow of information and the value of enhanced privacy protection, and to act on that choice by choosing among businesses offering different privacy protections. Choice would therefore require that consumers have the ability to choose among competing privacy policies, and obligates the government to preserve to the greatest degree possible a competitive market offering a variety of levels and means (and corresponding costs) of privacy protection. Viewed in this light, the choice principle is central to interpreting all of the other privacy principles.

c. Access

"Access" is the requirement that a business or other user of information provide an opportunity to the people about whom it collects or uses information to review that information. It is a component of some, but not all, pending privacy bills.[81] Virtually all access provisions include some opportunity to dispute the provenance, accuracy, or relevance of data, or to actually delete or amend offending data.[82]

For example, the FCRA requires consumer reporting agencies (often called credit bureaus) to provide consumers with a copy of their credit report upon request, and to do so without charge if the report was used as a basis of an adverse decision on credit, employment, or insurance.[83] Similarly, the FCRA implements critical dispute-resolution mechanisms. If a consumer disputes any data, the consumer reporting agency must investigate the claim and delete any disputed data that it cannot verify within 30 days, as well as notify recipients of credit reports contained disputed or inaccurate data of the change.[84] In addition, anyone who furnishes data to a credit reporting agency has a legal obligation to correct inaccurate data, notify any agency to which it

has reported data if it determines that those data are inaccurate, and disclose to any agency to which it is reporting data if the data's accuracy is disputed.[85] Other laws providing for consumer access to, and the opportunity to correct, personal information include the Family Education Rights and Privacy Act[86] (applicable to educational institutions receiving federal funds) and the Cable Communications Policy Act[87] (applicable to cable operators).

Despite the U.S. experience with limited access rights, broader access raises many issues. In February 2000, the FTC appointed a committee to study access and security issues in the context of online data collection and use. In May, the Commission's Advisory Committee on Online Access and Security published its final report, outlining the many unresolved issues surrounding access to and the opportunity to correct personal information, even when limited to the online context. Legislators should address these issues before adopting new access requirements:

- In what settings is access to be required—online, offline, or both?

- What type of access is to be provided—merely an opportunity to review information or the right to correct, amend, challenge, or delete information?

- How is access to be provided—online, by telephone, via the mail, or in person?

- When is access to be provided—immediately (in real time), only at specified intervals, upon request, in response to a specific event, annually, or on some other schedule?

- Some of the most difficult issues concern the personal information to which access must be provided. Information does not come labeled "personal." Would an "access and correct" law apply only to information that actually identifies an individual or would it apply to information that *could*, when combined with other data, identify a person? If the latter, is any information excluded? Does the source of the information matter—will access apply to information collected from one person about another? What if the information is observed rather than collected—would the access right, for example, apply to videotapes recorded by security cameras? What if it is collected from a third party—who must then provide access and to what information? What about information that is neither observed nor collected, but rather inferred or calculated—must access be provided to information that reflects a retailer's or other business' proprietary conclusions about a customer's interests or creditworthiness?

- Who must provide access and to whom must access be provided? Consider a simple retail transaction: A consumer uses a bank credit card to buy a gift which is then shipped to the recipient. The retailer collects personal information from the purchaser and about the purchaser when it verifies the credit card, and it may observe additional personal information through its security cameras and other means. Moreover, it records at least the name and address of the gift recipient, as well as what was sent to the recipient. The

bank issuing the credit card records the fact that the consumer has made a purchase and where. If a debit, rather than credit, card is used, the bank will also access the customer's account, verify the balance, and deduct the amount of the purchase. The shipper obtains the name and address of gift recipient and the value of the shipment. Now who gets access and an opportunity to correct, and from whom do they get it? Must the retailer provide access to the information obtained from the bank about the purchaser? (Recall that if the purchaser successfully corrects some inaccuracy in this information, that information is corrected only in the records of one end user—the retailer, and not in the records of the source of the information—the bank; the customer therefore has the illusion, but not the reality, of having corrected the information.) Must the retailer and the shipper provide access to the recipient of the gift, even though neither has any relationship with him or her? This simple example provides ample illustration of the complexity surrounding the questions of who must provide access and an opportunity to correct to whom.

- What triggers access? Can consumers file access requests with anyone they think may have personal information about them? Is access triggered if an entity merely possesses or uses personal information, but does not store it longer than necessary to complete the desired transaction? Or must any personal information, once obtained, be stored so that access can be provided? If so, this storage poses significant privacy concerns. Must access be provided to information that is unintelligible to the consumer (e.g., a proprietary credit score), or to information where no meaningful opportunity to correct exists (e.g., records of payments that have cleared or settled)? Must access be provided to information that does not pose any risk of harm or that is publicly available? In short, is access to be provided for its own sake or only when it serves some meaningful purpose? This fundamental question divided the FTC's Advisory Committee on Online Access and Security and its resolution is key to meaningful discussion of access and correction issues.

- This suggests that access without an opportunity to correct may be of little value. Yet there is a tremendous difference in both cost and risk associated with access combined with a right to amend, challenge, or delete disputed data. Must a business open its records to allow consumers to alter at will, or to remove information collected by the business as part of a transaction? Who wouldn't want to delete information about debts they owe or misdeeds they have committed? Yet if the right is more limited—for example, access and an opportunity to dispute the accuracy of data—how will disputes over accuracy be resolved, and by whom? Such a requirement seems rife for litigation.

- How will the law regulate access and assign the cost of providing it? Will the law set limits on access and correction requests? Will it restrict spurious claims? Who will pay for access—only those individuals seeking it or all consumers, through higher prices? Will the price of access be regulated and, if so, by whom and according to what standards?

- How does an entity required to provide access guarantee that it is providing access to the right person? This is an extremely complex concern, not just because of the difficulty of

authenticating identity, but because all of the measures currently available for doing so require that the individual provide *more* information about himself. Some access advocates suggest that users create a password when they first supply information to a business online. This approach is fraught with problems, not the least of which is few Internet users like to be bothered with creating a password for a single transaction and usually forget them even when they do. Moreover, the failure to create a password when the information is first supplied presumably makes future access impossible. Finally, this approach would only apply when the business first collects information directly from the data subject, as opposed to from a third party or observed from the data subject's behavior. The FTC's Advisory Committee on Online Access and Security was unable to resolve the authentication conundrum because it is inherent to providing access online. The resulting risk of providing access to, and an opportunity to correct, one individual's personal information to another individual is extremely disturbing to contemplate. Access would then become the perfect tool for identity theft, and the government that mandates access the unwitting accomplice of identity thieves.

- How can a right of access avoid requiring businesses to collect, store, and centralize more—as opposed to less—personal information? To maintain the tools necessary to authenticate the identity of an individual seeking access, businesses are likely to have to seek and store more personal information, such as a Social Security Number (SSN) or mother's maiden name. Even more troubling, many access proposals require that the business provide the consumer with online access to all of the personal information maintained about him or her, even if that information is not normally centralized or accessible via the Internet. For example, usage logs and back-up tapes usually contain information about individuals who browse a Web site, but this information may be used only in the event of a system failure, a dispute regarding a transaction, or, in the aggregate, to monitor and enhance system performance. If the law required access to all of this information, businesses would be compelled to bring together disparate sets of information—to engage in the very act of "profiling" that privacy advocates wish to restrict. Then they would need to make that new "super" database available via the Web and therefore subject to viruses and hackers. Some access proposals would even require that businesses retain personal information that they would otherwise destroy, just so they can provide access to it at a later date. All of these requirements have the effect of greatly increasing the volume, centralization, and vulnerability of personal data.

- How costly will access be? In addition to the potential costs to consumers in terms of greater data collection and the potential for wholesale identity theft, there is the risk of very real economic costs, reflected in reduced service and convenience and higher prices paid by consumers. The British Bankers' Association has calculated the cost of a single institution providing one customer with "a simple and straightforward report" under the EU data protection directive to be "in excess of £150"[88]—about $255 according to the exchange rates in effect at that time. The experience of the federal and state governments in the United States of complying with public sector access and privacy laws shows not

only that providing access costs hundreds of millions of dollars and consumes tens of thousands of worker hours each year, but also results in a high volume of litigation over the terms of access and the opportunity to correct information. Another, potentially greater, cost reflects the recognition that a substantial number of Americans today admit to cheating on their taxes, lying on résumés, exaggerating insurance claims, and otherwise deceiving their fellow citizens. Given these facts, is there any reason to suppose that access and an opportunity to seek correction of allegedly false information is going to be used to *increase* the accuracy of stored personal information or rather to *distort* that data to reflect the individual's preferences? All of the costs associated with requiring businesses to provide access and an opportunity to correct personal information are increased exponentially if that requirement is extended to providing access in the offline world and included information collected offline as well.

d. Security

Security, like access, has emerged in the present debate primarily in the online context, and is addressed by pending privacy bills.[89] "Security" refers to the obligation of data collectors and users to take reasonable precautions to protect those data from unauthorized access, transfer, alteration, or destruction. Although many of the steps necessary to satisfy the security principle are technological—the use of passwords, encryption, access logs, and the like—security is a much broader principle and incorporates far more than just software and hardware. It, too, is not without controversy, for a number of reasons that lawmakers should address:

- To the extent security does refer to technology, government-established standards intrinsically face the problem that digital technologies are changing rapidly and constantly. Any law or regulation that specified specific security measures would likely be out of date before it ever took effect. Therefore, the effect of such a law or regulation would be, at worst, to decrease the standard of security for stored data or, at best, to increase the cost of protecting those data.

- If the government does not establish a standard for security, however, few individuals are in a position to evaluate a security notice adequately. The FTC itself ran into this problem during its most recent survey of corporate Web policies. The Commission staff treated a Web site as having adequate security if it contained a policy saying that it did.[90] This does little to enhance consumer security.

- The greatest threat to the security of stored personal information is not the business that is maintaining the information, but rather the consumer who is providing it. For example, online security experts argue that the greatest threats to the security of most Internet transactions are the consumer disclosing his or her password or leaving his or her system logged on to a network. As a result, consumer education—rather than new laws—may be the most critical component of data security.

- Finally, many businesses argue that government regulation is least justified to protect the security of personal information because everyone involved in the responsible collection and use of such data shares a common interest in security. As much as any individual consumer fears harm if data are intercepted or wrongfully accessed, businesses stand to lose potentially more if their databases are "hacked" or accessed inappropriately. This is why businesses and other organizations have invested so heavily in security for the information they store.

The many issues raised by the four principles—notice, choice, access, and security—that dominate the current privacy debate reflect the tremendous complexity of government privacy protection and the fact that even when that protection is *procedural* on its face—purporting only to put rights into the hands of individuals—it nevertheless runs the risk of setting a de facto *substantive* privacy standard, and it does so without regard for the cost of overprotecting privacy or the risk of underprotecting it. This complexity highlights the compelling need for greater specificity in proposed laws and regulations. Only then can policymakers and the public evaluate the real impact of the proposed law or regulation, the extent to which it enhances individual control over privacy, and the costs that it imposes to do so.

4. Other Issues

a. Enforcement

Enforcement raises other issues, however, both because of the importance of ensuring that there is efficient, affordable enforcement privacy protections to be effective, and because of the risks associated with costly or duplicative enforcement mechanisms. Here, not surprisingly, there is a real division between most privacy advocates and most businesses. Privacy advocates argue that enforcement should be available through many venues—private law suits, class action law suits, federal and state agencies and law enforcement officials, and self-regulatory organizations—and that the goal of enforcement is not merely to correct errors but to provide dissuasive penalties to discourage future errors.

Businesses argue that extensive enforcement is needlessly costly, and especially when dealing with an area where the law, technologies, and markets are changing so rapidly. Many laws—ranging from the privacy provisions in Gramm-Leach-Bliley to general consumer protection laws such as Section 5 of the Federal Trade Commission Act[91]—already protect privacy. A single use of personal information can become the subject of dozens of enforcement actions brought under a variety of laws imposing a wide variety of requirements. For example, the decision by network advertiser DoubleClick to purchase consumer database company Abacus has resulted in investigations by the FTC and state attorneys general and in numerous individual and class action lawsuits. This type of enforcement scenario merely raises costs without aiding consumers or enhancing compliance. In addition, businesses contend that an additional strong incentive is hardly necessary, because they already face such significant penalties through lost customer confidence and intensive press scrutiny if they fail to live up to their own privacy policies or to protect their customers' information. Again, they point to DoubleClick, whose stock

value fell by 40% in a matter of weeks as a result of the *announcement* of an ill-considered plan to use consumer information.[92]

Another point of contention is the question of *harm*. Many uses of personal information that violate privacy laws or policies result in no tangible or economic harm to the individuals involved. In such a case, is the cost of private actions justified? Similarly, are multiple investigations and cases brought by the FTC and state attorneys general based on a single course of conduct justified? Business argue that where multiple legal requirements overlap, enforcement under all of those laws and regulations should take place through a single action.

b. Preemption

Preemption has also become a major topic in the current privacy debate. The states have played an historically important role in the development of laws, often serving as "laboratories" for legal regimes that are tested at the state level before being implemented nationally. Both privacy and free-flow advocates support preemption when they believe they can get a better deal from Congress than from the states, and oppose it when they calculate that the reverse is true. Congress has behaved inconsistently, preempting state regulation of information-sharing among affiliates in the 1996 amendments to the FCRA,[93] and compelling the states to comply with a federal privacy standard in the 1994 Drivers' Privacy Protection Act (DPPA)[94] and the Shelby Amendment to the 1999 Transportation Appropriations Act,[95] but specifically permitting stronger state regulation of financial and health privacy in Gramm-Leach Bliley[96] and the HIPAA regulations.[97] Only one of the privacy bills currently before Congress includes a preemption provision.[98]

Calculations of immediate political advantage aside, it seems clear that commerce in this country is predominantly national and, especially with the advent of the World Wide Web, global. Many businesses operate in multiple states and would be greatly burdened by the obligation to comply with inconsistent privacy obligations. Moreover, consumers are increasingly mobile and, even those who live and work in a single state, increasingly obtain products and services from across state lines. In addition, the exponential growth in online commerce means not only that more consumers are making purchases via the Internet, but that online and offline transactions are increasingly interconnected.

If consumers are to be served effectively and efficiently, privacy rules need to apply across technological contexts and geographic boundaries. Privacy advocates often complain of the "patchwork" nature of federal privacy law, but 51 sets of divergent state laws only exacerbate this situation, while increasing the cost and burden of privacy protection to both consumers and businesses. This suggests that, except in areas that are truly intrastate and therefore should remain within the purview of states, laws that are necessary to enhance consumer privacy protection should be national in scope, and should preempt state laws on the same subject matter. States would continue to play a critical role in advising the federal government on privacy issues and

sharing enforcement authority with federal agencies under federal privacy laws.[99] Consumers in the global information economy are ill-served by any other approach.[100]

THE COST OF PRIVACY LAWS AND REGULATIONS

Even while participants in the privacy debate disagree over the proper role of government in protecting privacy, there is almost universal consensus that privacy laws should, on balance, generate greater benefits than costs. Laws designed to protect privacy should impose no cost that does not achieve commensurate increases in privacy protection.

We have already seen the potential costs associated with interfering with beneficial flows of information. Before enacting privacy laws, lawmakers need to balance the value of the privacy protection that those laws facilitate with the cost of interfering with the benefits that result from robust information flows. This requires considering both the extent to which the law facilitates privacy and the extent to which it interferes with valuable information flows. For example, California, in an effort to protect privacy, prohibited the use of arrestee addresses obtained from law enforcement agencies for marketing products or services, but explicitly permitted such information to be used for "journalistic" purposes.[101] It is difficult to imagine that arrestee privacy was materially advanced by prohibiting attorneys and private investigators from sending a letter offering their services, while permitting a newspaper to publish the names and addresses of arrestee in the newspaper. At the same time, it is easy to see that prohibiting attorneys and private investigators from offering their services to arrestees might materially harm those arrestees, while the benefits of allowing a newspaper to publish arrestee addresses is less clear. This "overall irrationality," as Justice Stevens called it in his dissent from the Supreme Court's decision upholding the constitutionality of the statute on other grounds, "eviscerate[s] any rational basis for believing that the Amendment will truly protect the privacy of these persons."[102]

In addition, there are other costs that must be considered, such as the cost to both consumers and businesses of complying with the law. For example, Gramm-Leach-Bliley requires financial institutions to "clearly and conspicuously" provides consumers with a notice about its policies and practices for disclosing personal information. That disclosure must be made "[a]t the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship."[103] By June 12, 2001, approximately 40,000 financial institutions will be sending as many as 2.5 billion notices to their various customers. Households will receive an average of 20-50 notices each. Printing and mailing costs alone will be in the $2 to $5 billion range, if not more. Internal compliance costs are much higher. A rational inquiry would ask whether consumer privacy is materially advanced by this annual onslaught of legal notices, and, if so, whether that benefit is worth the multi-billion dollar price tag or whether the same degree of privacy protection could have been achieved by requiring financial institutions to prominently post their privacy notices or make them available to customers without charge upon request.

Similar questions are raised by the recent final rules on health privacy released by the Department of Health and Human Services (HHS) under HIPAA.[104] The rules establish a control-based system under which a health care provider or insurer may not use oral or recorded information about an individual's health, treatment, or payment for health care without the individual's express consent.[105] The goal may be laudable, and certainly many Americans consider health information to be among the most sensitive types of data, but the potential cost to consumers and companies raises significant questions about whether the rules are the best way to protect health privacy. Just the required elements of the mandatory notice that must be given to consumers before information can be collected or used are calculated to run nine pages. Although the rules are based entirely on consent, they apply to deceased individuals.[106] In addition, for information to be considered "de-identified"—so that it can be used for medical research without complying with the extensive consent requirements—the information must contain no reference to location more specific than a state (or first three digits of a zip code if certain other requirements are met) and no reference to a date more specific than a year.[107]

HHS calculates cost of complying with these rules at $3.2 billion for the first year, and $17.6 billion for the first ten years.[108] Based on the prior, less complicated draft of the rules, health care consulting companies have calculated that the cost will be much higher—between $25 and $43 billion (or three to five times more than the industry spent on Y2K) for the first five years for compliance alone, not including impact on medical research and care or liability payments.[109]

But cost is not only measured in economic terms. The restrictive privacy provisions of the HIPAA regulations also threaten medical research and the development of new drugs and treatments. As a result, those regulations threaten the quality of care for everyone. Helena Gail Rubinstein has written that privacy advocates refuse to recognize "in exchange for the vast improvements in medical care, a correlative responsibility on the part of the individual, as a consumer of health care services, toward the community. As individuals rely on their right to be let alone, they shift the burden for providing the data needed to advance medical and health policy information. Their individualist vision threatens the entire community . . . ."[110]

There is no question but that health privacy is important and should be protected as a matter of law. The issue raised by these rules, however, is whether health privacy can be protected as effectively, or even more effectively, at lower cost. That cost is measured not only in economic terms, but in consumer convenience (one family member could no longer pick up a prescription for another family member, because each individual must sign his own consent form), and in potential harm to medical research and innovation.

Finally, lawmakers need to ensure that laws intended to enhance privacy protection do not diminish or interfere with existing privacy protection. For example, some legislators have introduced bills designed to prevent identity theft by restricting the use and disclosure of SSNs.[111] This highlights the conundrum that efforts to prevent identity theft inherently pose. One of the major issues concerning identity theft today is how to accurately separate data about one individual from data about another. This is made all the more difficult by the fact that

approximately 16% of the U.S. population—about 42 million Americans—changes addresses every year; there are approximately 2.4 million marriages and 1.2 million divorces every years, often resulting not only in changed addresses, but also in changed last names; and, as of 1998, there were 6 million vacation or second homes in the United States, many of which were used as temporary or second addresses.[112]

The only reliable way to date to ensure that information about one consumer is not erroneously provided to another consumer or added to another consumer's file is to organize those files by SSN. Just a single segment of the modern economy—consumer reporting agencies, i.e., credit bureaus—processes 2 billion pieces of personal data on 180 million active consumers every month. Identifying those data by SSN (together with other personal information) is the only reliable way of ensuring that they are attributed to the right person. Yet this is precisely what proponents of legislation designed to restrict the use of SSNs want to stop.

Similarly, many businesses are expanding their account monitoring to detect fraud. Yet a number of pending privacy laws threaten to restrict the ability of merchants to use this identity theft detection strategy or to condition account monitoring on consumer consent. As a result, the government becomes the unwitting accomplice of identity thieves.

Enacting laws that restrict information without enhancing privacy protection or that fail to anticipate and explicitly consider the cost of privacy protection hurts consumers, businesses, and the entire economy.

THE CONSTITUTIONALITY OF PRIVACY LAWS AND REGULATIONS

The impact of the Constitution on government privacy protections has also proved a subject of controversy in the current privacy debate. It warrants close attention as no law or regulation can be allowed to stand if it violates constitutional provisions. Legislators must therefore determine not only that a privacy law generates more benefits than costs, but also that it does so in a manner consistent with the Constitution.

Regulators and privacy advocates have argued that there is a constitutional right to privacy. The introduction to the recent HIPAA health privacy rules, for example, discusses at length the Fourth Amendment right to be free from "unreasonable searches and seizures" and the right to informational privacy recognized by the Supreme Court in *Whalen v. Roe*,[113] involving a New York statute that created a state database of persons who obtained certain prescription drugs. Unfortunately, the rules' drafters failed to note that both the Fourth Amendment and the right identified in *Whalen*, as with all constitutional rights, apply only against the *government*. The *government* may not unreasonably search and seize and the *government* may not compel disclosure of personal matters in certain circumstances. The private sector, by contrast, is free to do so, at least from a constitutional perspective. Moreover, even in the context of government collection and use of information, the Supreme Court has never found that any collection or use of personal information violated the right to informational privacy. In *Whalen*, the Supreme Court scrutinized the New York State law under an intermediate level of scrutiny, rather than apply the

strict scrutiny reserved for laws touching on "fundamental" interests, and ruled that the government was permitted to collect the information it sought.

While there is clearly no federal constitutional right to privacy that requires or supports government action to protect privacy in the market, any such action that the government does take must be consonant with the First Amendment if it is to survive constitutional review.

The Supreme Court has decided many cases in which individuals sought to stop, or obtain damages for, the *publication* of private information, or in which the government restricted *expression* in an effort to protect privacy. Virtually without exception, the Court has upheld the right to speak or publish or protest under the First Amendment, to the detriment of the privacy interest. For example, the Court has rejected privacy claims by unwilling viewers or listeners in the context broadcasts of radio programs in city streetcars,[114] R-rated movies at a drive-in theater,[115] and a jacket bearing an the phrase "Fuck the Draft" worn in the corridors of a courthouse.[116] As noted, the Court has struck down ordinances that would require affirmative consent before receiving door-to-door solicitations,117 before receiving Communist literature,[118] even before receiving "patently offensive" cable programming.[119] Plaintiffs rarely win suits brought against speakers or publishers for disclosing private information. When information is true and obtained lawfully, the Supreme Court has repeatedly held that the government may not restrict its disclosure without showing a very closely tailored, compelling governmental interest—the highest level of constitutional scrutiny. Under this requirement, the Court has struck down laws restricting the publication of confidential government reports,[120] and of the names of judges under investigation,[121] juvenile suspects,[122] and rape victims.[123]

Even if the information is considered to be "commercial," its publication is nevertheless protected by the First Amendment. The Supreme Court has found that such expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a "substantial" public interest, the intrusion "directly advances" that interest, and is "narrowly tailored to achieve the desired objective."[124]

However, the Supreme Court has not yet decided a case in which a party sought to apply the First Amendment to overturn a privacy law or regulation that restricted the *collection* of personal information in the market, but did not otherwise restrain publication or expression. It is therefore unclear how the Court might evaluate the constitutionality of such a law. One likely reason that the Court has not yet confronted such a law is the practical reality that few if any privacy laws restrain only the *collection* of personal information. Instead, virtually all privacy laws also limit the *use* of that information. Where that use involves expression, either to the individual data subject or to a third party, the Court would almost certainly subject the law to close scrutiny under the First Amendment.

This is precisely what the Tenth Circuit did when presented with a First Amendment challenge to FCC rules that required U.S. West to get "opt-in" consent from customers before using data about their calling patterns to determine which customers to contact or what offer to

make them.[125] The appellate court found that the FCC's rules, by limiting the use of personal information when communicating with customers, restricted U.S. West's speech and therefore were subject to First Amendment review. The court then determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were "'no more extensive than necessary to serve [the stated] interests.'"[126] Finally, the court found that the FCC had failed to meet this burden and therefore struck down the rules as unconstitutional. The Supreme Court declined to review the case.[127]

Although not directly applicable, the Supreme Court's Fourth Amendment jurisprudence is also instructive. Even in the face of an explicit constitutional command to protect individuals from government intrusions, the Court has long held that the constitutional protections for privacy only protect *reasonable* expectations of privacy. When evaluating wiretaps and other seizures of private information under the Fourth Amendment, the Supreme Court has long asked whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experience and widely shared community values.[128] Similarly, virtually all state privacy torts—with the sole exception of commercial appropriation—require that the invasion of privacy be *outrageous* or *unreasonable*.[129] The Supreme Court has struck down laws that did not contain such a requirement.[130]

What can be said, then, about the current state of constitutional law applicable to privacy protection is that the Constitution requires that the government protect privacy only from *government* intrusion, and even then only from unreasonable intrusions. The Constitution restrains the government from enacting privacy protections applicable to the private sector that restrict information flows. And, while the applicability of that constitutional restraint to laws restricting the collection or use of personal information for purposes other than publication has not been definitively resolved by the Supreme Court, the Court's prior cases involving privacy claims in other contexts suggest that the Court will look with disfavor on privacy laws that interfere with expression, protect more than reasonable expectations of privacy, fail to respond to *specific harms*, or impose costs without commensurate benefits to the public.

THE IMPORTANCE OF CONTEXT

One of the most important lessons learned from recent privacy laws and regulations, and one of the most significant causes of those enactments underprotecting or overprotecting privacy or imposing unnecessary costs, is the importance of context. Privacy laws are most burdensome and least effective when they apply broadly, without proper concern for the settings in which they will operate, the types of information they cover, the obligations that they impose, and the purposes they were designed to serve. Legislators are therefore wise to scrutinize proposed privacy laws to determine how well tailored they are to the contexts in which they will operate. Although there are many specific contextual factors to consider, the following have emerged as among the most significant:

- Is the law or regulation intended to apply online, offline, or both? Each setting presents its own unique issues. For example, it is easier to collect data and to do so

without the individual knowing it online, but it is also easier to provide conspicuous notice and access online. Technologies play a useful role in protecting privacy online, but comparatively little offline.

- Is the law or regulation intended to restrict all uses of information or merely harmful ones? Recent privacy enactments have been prompted by specific incidents of harmful use of information, but then they have been applied to all uses, no matter how innocuous. While such broad laws may enhance consumer control, their breadth means that they do so at a high price and with the potential risk of diminishing the level of privacy protection by inundating consumers with privacy notices and consent forms. Even worse, some recent laws fail to regulate the harmful activity that motivated their creation. The 1994 DPPA, which restricts the disclosure of name and address information from motor vehicle records,[131] was enacted in response to the 1989 murder of actress Rebecca Schaeffer, who was stalked by an obsessed fan using information provided by a private investigator from her California Department of Motor Vehicles record. While the law restricts the *public*'s access to motor vehicle records, it does not restrict that of private investigators.

- To what information does the law or regulation apply? Historically, privacy interests were thought to be at stake only when personal information was involved. Publicly available information or information that consumers routinely and freely disclosed was not thought worth the cost of protecting. This is no longer the case. Federal financial regulators have interpreted Gramm-Leach-Bliley to apply to "any information" provided to a financial institution "to obtain a financial product or service," "[a]bout a consumer resulting from any transaction involving a financial product or service," or that the financial institution "otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer."[132] It is not necessary that the information be "financial" or even "personally identifiable." HIPAA, too, follows this trend of applying the law to a broad range of information, including oral information.[133] And, as already noted, NAAG has proposed requiring "opt-out" consent for permission to use data that are not personally identifiable.[134] The further that legal enactments move beyond private or sensitive information to extend to all information about an individual or even information that is not about an identifiable individual, the greater the cost and burden that those enactments are likely to impose.

- Another important contextual factor is whether the information collection and use is visible or surreptitious. Providing formal notice and seeking consent in a setting in which it is clear that the data subject knows she is providing information and for what purpose is not only likely to prove an unnecessary expense, but also an annoyance. On the other hand, providing notice when the data subject would ordinarily have no idea that information is being collected seems more likely to be a necessary requirement for meaningful privacy protection.

- A similar distinction exists between laws and regulations applicable to information collection *from* the data subject and information collection *about* the data subject. When collecting information directly from the data subject, it is generally easier and less costly to provide notice and seek consent, even though it may be less necessary if the data collection is clear. Requiring notice and consent when acquiring information about a data subject from a third party is almost always more costly, if not impossible, but it may also be more necessary if the data subject would not otherwise know of the activity. Historically the law has dealt with the third-party situation through general education or notices provided after the fact, for example, in the first solicitation sent using the information. More recent laws and regulations have been less cognizant of this distinction, however, and have imposed the same notice and consent requirements irrespective of the source of the information.

- Another important contextual factor is whether the person to whom the information pertains is a child or an adult. In 1999, the FTC adopted stringent online privacy protections for data collected from children.[135] Some lawmakers have suggested extending those rules to adult Internet users. To do so would ignore the fact that heightened protections and costs that might be justified to protect children might not be justified in the case of adults.

- Whether the context is public or private is another important factor. Historically, courts have accorded little if any privacy protection to activities that were observed in public. On the other hand, conduct that took place in a private setting, such as a bedroom, was often found more deserving of protection. Today, that distinction may be breaking down as privacy protections are extended to publicly available information, disclosures made in e-mail or online chat rooms (the technological equivalent of post cards or bulletin boards in public hallways), or on someone else's premises, such as an employer's computer. Clearly, some protection in even these settings may be justified, but the cost of privacy protections go up as they are extended outside of private settings, and the justification for them arguably decreases.

- Is the data collection and use by a government agency or by a private actor? This is a critical distinction for determining the constitutionality of a proposed law or regulation, but it also raises many practical issues about the power of the individual to decline to provide the data or to seek a product or service from a competing provider. Many recent privacy enactments have blurred the distinction. In fact, some, like the HIPAA privacy regulations, actually reduce the level of protection accorded information from government collection and use, while greatly increasing the protection against private sector collection and use.

- Does a privacy enactment apply only to the commercial collection and use of data, or does it also apply to political campaigns, religious groups, charities, membership organizations, and other not-for-profit groups? Interestingly, few legislative proposals

> would apply to the not-for-profit community, although it seems clear that these groups are significant users of personal information and the risk to individuals that the collection and use of such information poses—however great or small it may be—does not depend upon whether the use is for profit or not. A political campaign sharing the party affiliation of a voter or a not-for-profit group marketing based on the age of a potential member is no less invasive of personal privacy than a financial institution marketing a product or service to customers based on their likely interest and eligibility.

Obviously, there are other contextual issues, and they are clearly interrelated. A law that applies to all uses of all information, both online and offline, including information collected visibly and in public settings, is far more likely to impose higher costs and burdens on consumers and businesses than a law with a narrower scope. Because that broad law also extends to information that is neither sensitive nor private, and requires compliance with regulatory formalities where the collection of information is clear, those costs are less likely to be justified and the law is less likely to survive a constitutional challenge. Similarly, if that same law can be tailored to apply only to information that is sensitive or reasonably viewed as private, and only restricts harmful use rather than any use, it is more likely to provide efficient, effective, and constitutional privacy protection.

CONCLUSION: THE GOALS OF PRIVACY PROTECTION

Legislators play a critical role in helping to protect the privacy of every individual. One of the most important responsibilities of the government is assuring that its own house is in order. Only the government has the power to compel disclosure of personal information and only the government operates free from market competition and consumer preferences. As a result, the government has special obligations to ensure that it complies with the laws applicable to it; collects no more information than necessary from and about citizens; employs consistent, prominent information policies through public agencies; and protects against unauthorized access to citizens' personal information by government employees and contractors.

Similarly, there are many steps that only the government can take to protect citizens against privacy-related harms, such as identity theft: Make government-issued forms for identification harder to obtain; make the promise of centralized reporting of identity thefts a reality; make it easier to correct judicial and criminal records and to remove permanently from one individual's record references to acts committed by an identity thief. The government alone has this power.

Regulators and law enforcement officials should enforce existing privacy laws vigorously, and legislators should ensure that they have the resources to do so. As we have seen, existing federal and state laws create significant legal authority for public investigation and enforcement. Before asking for more authority, the government should ensure that what exists is already used effectively.

The various arms of the government should also work together, and with public schools and universities, private industry, and not-for-profit groups, to educate the public about privacy and the tools available to every citizen to protect her own privacy. Citizens need to know about the 800-numbers they can call to be removed from mailing lists and prescreened offer lists, how to use the technology already in Internet browsers to protect against unwanted profiling and data collection, and about the steps they can take to protect their own privacy. Individuals alone control many privacy protection mechanisms—no other entity may make these decisions for them. Yet, without education, most individuals fail to recognize the importance of their responsibility or lack the knowledge to fulfill it.

Many of these points have been lost in the legislative and regulatory focus and heat of the current privacy debate, which is unfortunate because not only do these steps together yield greater privacy protection than virtually any law, but there is nearly universal agreement as to their importance.

When new laws or regulations are thought necessary, it is critical to clearly identify and articulate what purpose a proposed privacy law or regulation is intended to serve and whether it will in fact prevent or remedy that harm: In sum, what public benefit justifies the government's action? Only after having answered this question can the benefits of the proposed law or regulation be balanced against both the beneficial uses of information with which it interferes and the other costs of implementing and complying with the law. Armed with this information, lawmakers can then ask whether the law is worth its cost or whether there are other less intrusive, less expensive, or more effective tools for achieving the same purpose. Finally, lawmakers must determine that the law is constitutionally permissible. In answering all of these questions, consumers, businesses, and rational lawmaking all benefit from a close and careful scrutiny of the specific requirements of the proposed law or regulation and the specific privacy contexts in which it will operate.

As the intensity of the current privacy debate suggests, privacy is a highly complex, difficult subject that affects every person. To treat it as any less complicated or any less important threatens the convenience, service, recognition, and opportunity that consumers enjoy as the result of information-sharing, and the information infrastructure that undergirds our economy and our democracy.

NOTES

APPENDIX

Participants in the American Enterprise Institute's Privacy Roundtable
November 17, 2000

Marty Abrams
Executive Director
Center for Information Policy Leadership @ Hunton & Williams

Stewart A. Baker
Steptoe & Johnson LLP

Jerry Berman
Executive Director
Center for Democracy and Technology

Fred H. Cate
Visiting Scholar
American Enterprise Institute;
Professor of Law
Indiana University School of Law—Bloomington

Susan Grant
Vice President, Public Policy
Director, National Fraud Information Center/Internet Fraud Watch
National Consumers League

Julia E. Johnson
Director
Office of Information Practices & Privacy
Bank One Corporation

Gina Keeney
Chief Policy Counsel
Dell Government Relations

Jane Kirtley
Silha Professor of Media Ethics and Law
School of Journalism and Mass Communication
University of Minnesota

Walter Kitchenman
TowerGroup

Alan Charles Raul
Sidley & Austin

Paul M. Schwartz
Professor of Law
Brooklyn Law School

Solveig Singleton
Senior Analyst
Project on Technology & Innovation
Competitive Enterprise Institute

Michael E. Staten
Distinguished Professor and Director
Credit Research Center
Georgetown University

Peter J. Wallison
Resident Fellow and Codirector,
Financial Deregulation Project
American Enterprise Institute

Affiliations provided for identification purposes only.

---

1. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* 16 (May 2000) (Commissioner Orson Swindle, dissenting).

2. Gramm-Leach-Bliley Financial Services Modernization Act tit.V, 106 Pub. L. No. 102, 113 Stat. 1338 (1999) (codified at various sections of 15 U.S.C.).

3. Department of Transportation and Related Agencies Appropriations Act, Pub. L. No. 106-69, § 350, 113 Stat. 986, 1025-26 (1999).

4. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

5. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (FTC, final rule) (codified at 16 C.F.R. pt. 312).

6. Robert O'Harrow, Jr., "A Postscript on Privacy; Bank Bill's Late Change Gives States Last Word," *Washington Post*, Nov. 5, 1999, at E1; Marcy Gordon, "States Challenge Information-Sharing in New Banking Measure," *Commercial Appeal* (Memphis, TN), Nov. 6, 1999, at C1.

7. Federal Trade Commission, *Online Profiling: A Report to Congress (Part 2)—Recommendations* (July

2000); Federal Trade Commission, *Privacy Online*, supra.

8. Reno v. Condon, 528 U.S. 141 (2000); Los Angeles Police Department v. United Reporting, 528 U.S. 32, 44 (1999) (Stevens, J., dissenting).

9. S. 30 (Financial Information Privacy Protection Act of 2001), 107th Cong. (2001); S. 290 (Student Privacy Protection Act), 107th Cong. (2001); S. 318 (Genetic Nondiscrimination in Health Insurance and Employment Act), 107th Cong. (2001); S. 324 (Social Security Number Privacy Act of 2001), 107th Cong. (2001); H.R. 89 (Online Privacy Protection Act of 2001), 107th Cong. (2001); H.R. 91 (Social Security Online Privacy Protection Act), 107th Cong (2001); H.R. 112 (Electronic Privacy Protection Act), 107th Cong. (2001); H.R. 220 (Identity Theft Protection Act of 2001), 107th Cong. (2001); H.R. 237 (Consumer Internet Privacy Enhancement Act), 107th Cong. (2001); H.R. 260 (Wireless Privacy Protection Act of 2001), 107th Cong. (2001); H.R. 347 (Consumer Online Privacy and Disclosure Act), 107th Cong. (2001); H.R. 583 (Privacy Commission Act), 107th Cong. (2001); H.R. 602 (Genetic Nondiscrimination in Health Insurance and Employment Act), 107th Cong. (2001);

10. Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data, 66 Fed. Reg. 9339 (Feb. 7, 2001) (FTC, notice).

11. National Association of Attorneys General, *Draft Statement on Privacy Principles and Background* (Dec. 11, 2000).

12. Kent Walker, "Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange," *Stanford Technology Law Review* ¶ 15 (2001) <http://stlr.stanford.edu/stlr/articles/00_stlr_2>.

13. Christine Harvey, "American Opinion (A Special Report): Optimism Outduels Pessimism," *Wall Street Journal*, Sept. 16, 1999, at A10.

14. Matthew Greenwald & Associates, Views on Privacy and the Sharing of Financial Information Between Business Partners Among Voters in Five States 3 (2000).

15. See "The Information Infrastructure" and "The Constitutionality of Privacy Laws and Regulations," infra.

16. 15 U.S.C. § 1681b(a) (1999).

17. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O.J. 95/L281), art. 26(1).

18. Alan F. Westin, *Privacy and Freedom* 7 (1967).

19. Enactment of the Children's Online Privacy Protection Act, 106th Congress, 2d Session, 146 Cong. Rec. E616, May 2, 2000, statement of Jay Inslee (D-Wash.) (emphasis added).

20. Democrats Hold News Conference on Financial Privacy, May 4, 2000 (statement of John LaFalce (D-N.Y.)) (emphasis added).

21. National Association of Attorneys General, supra at 7 (emphasis added).

22. S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong.§ 2(b)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001) (emphasis added)

23. See, e.g., United States v. Miller, 425 U.S. 435 (1976).

24. See "The Constitutionality of Privacy Laws and Regulations," infra.

25. See "The Information Infrastructure," infra.

26. Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (1997).

27. Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns* 1 (The Tower Group 1999).

28. Consumer Bankers Association, *1998 Automobile Finance Study* at 19.

29. Kitchenman, supra, at 7.

30. Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Banking and Financial Services, July 21, 1999 (statement of Edward M. Gramlich).

31. Barry Flynn, "In Search of Security, Some Banks Are Giving the Thumbs up to Fingerprinting New Customers," *Orlando Sentinel*, March 2000, at B1; Steven Marjanovic, "Banks Tap ATM Systems To Banish 18B Checks," *American Banker*, June 14, 2000, at 1.

32. Gary Fields, "Victims of Identity Theft Often Unaware They've Been Stung," *USA Today*, March 15, 2000, at 6A (quoting Undersecretary James Johnson of the U.S. Treasury Department).

33. "Insurance Fraud," *III Insurance Issues Update*, Oct. 2000.

34. General Accounting Office, *Medicare Improper Payments: While Enhancements Hold Promise for Measuring Potential Fraud and Abuse, Challenges Remain* (GAO/AIMD/OSI-00-281) at 4 (2000).

35. Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse* <http://www.cfenet.com/newsandfacts/fraudfacts/reporttothenation/reportsection4.shtml>.

36. Monitor Patriot Co. v. Roy, 401 U.S. 265 (1971).

37. Bill Pryor (R-Ala.), *Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium*, July 11, 2000, Washington, DC, at 4.

38. Edmund Sanders, "Your Bank Wants to Know You," *Los Angeles Times*, Dec. 23, 1999, at A1.

39. See "Choice," infra.

40. Brief for Petitioner and Interveners at 15-16, U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

41. Hearings before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Senate Comm. on Appropriations, March 24, 1999 (statement of Louis J. Freeh).

42. Hearings before the House Committee on Banking and Financial Services, July 28, 1998 (statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis).

43. See "The Role of Law," infra.

44. See, e.g., H.R. 91, 107th Cong (2001); H.R. 220, 107th Cong. (2001).

45. Identity Theft, Hearings before the Subcomm. on Telecommunications, Trade & Consumer Protection and the Subcomm. on Finance and Hazardous Materials of the House Committee on Commerce, April 22, 1999 (statement of Charles A. Albright, Chief Credit Officer, Household International, Inc.).

46. See "Self-Regulation" and "The Role of Law," infra.

47. 47 C.F.R. § 64.1200(e)(2).

48. 15 U.S.C. § 1681b(c)(5).

49. 106 Pub. L. No. 102, 113 Stat. 1338, tit. V (1999).

50. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* at 11 (2000).

51. General Accounting Office, *Federal Agencies' Fair Information Practices* (GAO/AIMD-00-296R) at 3 (2000).

52. Memorandum from OMB Director Jack Lew (Memorandum M-99-18) (June 2, 1999).

53. Darrell M. West, *Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments* (Sept. 2000) <http://www.brown.edu/Departments/Taubman_Center/polreports/egovtreport00.html#Security, Privacy and Disability Access>.

54. Direct Marketing Association, *Name Removal Services* <http://www.the-dma.org/home_pages/consumer/dmasahic.html#removal>.

55. Federal Trade Commission, *Individual Reference Services: A Report to Congress* (1997).

56. See <http://www.networkadvertising.org/>; Federal Trade Commission, *Online Profiling: A Report to Congress* (June 2000); Federal Trade Commission, *Online Profiling: A Report to Congress—Part 2: Recommendations* (July 2000); Network Advertising Initiative, *Self-Regulatory Principles for Online Preference Marketing by Network Advertisers* <http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf>.

57. See <www.truste.org>.

58. See <www.BBBOnLine.org/>.

59. See "Enforcement of 'Voluntary' Undertakings," infra.

60. 42 U.S.C. §§ 2000e, 2000e-2(a) (1997).

61. Id. §§ 3601, 3604-06.

62. 15 U.S.C. § 57b-1.

63. See, e.g., S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong.§ 2(b)(1) (2001); H.R. 112, 107th Cong. § 2(b)(1)(B) (2001); H.R. 237, 107th Cong. § 2(a)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001).

64. 15 U.S.C. § 503.

65. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

66. Ted Kemp, "Privacy Flap Cuts The Click In DoubleClick," *InternetWeek*, Dec. 18, 2000.

67. 15 U.S.C. §§ 1681-1681t.

68. 15 U.S.C. § 503.

69. National Association of Attorneys General, supra at 10.

70. 45 C.F.R. § 164.502.

71. See, e.g., S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong.§ 2(b)(1) (2001); H.R. 112, 107th Cong. § 2(b)(1)(B) (2001); H.R. 237, 107th Cong. § 2(a)(2) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001).

72. Less than 3% of the U.S. population takes advantage of the Direct Marketing Association's Mail and Telephone Preference Services. Financial Privacy, Hearings Before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Banking and Financial Services, July 20, 1999 (statement of Richard A. Barton); see also *Personalized Marketing and Privacy on the Net: What Consumers Want, A Privacy & American Business Consumer Privacy Survey Questionnaire* (Development and Report by Dr. Alan F. Westin, Fieldwork and Data Preparation by Opinion Research Corporation) (Nov. 1999).

73. Congressional Briefing on Internet Privacy: The Role of Government and Industry in Providing Consumer Empowerment, IT Congressional Working Group and Information Technology Association of America, Washington, DC, June 8, 2000 (statement of Robert Pitofsky).

74. 45 C.F.R. § 164.508(b)(4).

75. See "The Constitutionality of Privacy Laws and Regulations," infra.

76. U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 120 S. Ct. 1240 (2000) (emphasis added).

77. Martin v. Struthers, 319 U.S. 141 (1943).

78. Lamont v. Postmaster General, 381 U.S. 301 (1965).

79. Denver Area Educational Telecommunications Consortium, Inc. v. FCC, 518 U.S. 727 (1996).

80. 319 U.S. at 141.

81. See, e.g., S. 30, 107th Cong. § 6 (2001); H.R. 89, 107th Cong.§ 2(b)(1)(B)(ii) (2001).

82. See, e.g., Federal Trade Commission, *Privacy Online*, supra.

83. 15 U.S.C. § 1681m.

84. Id. § 1681i.

85. Id. § 1681.

86. 20 U.S.C. § 1232.

87. 47 U.S.C. § 551.

88. *The Home Office Consultation Paper on the Implementation of the EU Data Protection Directive—The British Bankers' Association Response, Annex I* (Costs).

89. See, e.g., H.R. 89, 107th Cong.§ 2(b)(2)(C) (2001); H.R. 237, 107th Cong. § 2(b)(1)(F) (2001)

90. Federal Trade Commission, *Privacy Online*, supra at 18-19.

91. 15 U.S.C. § 45(a).

92. Ted Kemp, supra.

93. The Consumer Credit Reporting Reform Act of 1996, Pub. L. No. 104-208, § 624, 110 Stat. 3009 (1996) (codified at 15 U.S.C. § 1681t).

94. Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).

95. Department of Transportation and Related Agencies Appropriations Act, 2000, § 350, 106 Pub. L. No. 69, 113 Stat. 986 (1999).

96. 15 U.S.C. §§ 507(a), 524(a).

97. 45 C.F.R. §§ 160.202-160.203.

98. H.R. 237, 107th Cong. § 2(c) (2001).

99. State attorneys general share enforcement authority with the FTC under the Telemarketing Sales Rules, 16 C.F.R. § 310.7., and the Fair Credit Reporting Act, 15 U.S.C. § 1681s(c).

100. For a recent and contrasting discussion of the role of states in protecting privacy see Bruce H. Kobayashi & Larry E. Ribstein, *State Regulation of Consumer Marketing Information* (forthcoming from the American Enterprise Institute).

101. Cal. Gov't Code § 6254(f)(3).

102. Los Angeles Police Department v. United Reporting, 528 U.S. 32, 44 (1999) (Stevens, J., dissenting).

103. 15 U.S.C. § 503(a).

104. 45 C.F.R. pt. 160.

105. Id. §164.502.

106. Id. §164.502(f).

107. Id. §§164.514(b)(2)(i)(B)-(C).

108. 65 Fed. Reg. 82,761, table 1.

109. Robert E. Nolan Company, Inc., *Common Components of Confidentiality Legislation—Cost and Impact Analysis* (1999); Fitch IBCA, *HIPAA: Wake-Up Call for Health Care Providers* (2000); Barbara Kirchheimer, "Report Predicts Huge HIPAA Price Tag," Modern Healthcare, Oct. 2, 2000, at 48.

110. Helena Gail Rubinstein, "If I am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate," 25 *American Journal of Law and Medicine* 203 (1999).

111. See, e.g., S. 324, 107th Cong. (2002); H.R. 91, 107th Cong (2001); H.R. 220, 107th Cong. (2001); H.B. 41 (Ark. 2001); H.B. 48 (Ark. 2001); S.B. 49 (Ark. 2001); H.B. 2320 (Ariz. 2001); A.B. 60 (Cal. 2001); H.B. 5307 (Conn. 2001); S.B. 422 (Conn. 2001); H.B. 361 (Haw. 2001); H.B. 31 (Iowa 2001); H.B.

46 (Iowa 2001); H.B. 147 (Ill. 2001); H.R. 4 (Ill. 2001); H.B. 2117 (Ind. 2001); H.B. 642 (Mass. 2001); H.B. 1163 (Mass. 2001); H.B. 2744 (Mass. 2001); H.B. 80 (Me. 2001); S.B. 92 (Mo. 2001); H.B. 388 (Mont. 2001); H.B. 262 (Mont. 2001); H.B. 282 (Mont. 2001); S.B. 262 (Mont. 2001); H.B. 1174 (N.D. 2001); H.B. 1245 (N.D. 2001); L. 106 (Neb. 2001); L. 239 (Neb. 2001); L 330 (Neb. 2001); L. 565 (Neb. 2001); L. 656 (Neb. 2001); S.B. 727 (N.J. 2001); S.B. 2003 (N.J. 2001); A.B. 16 (N.Y. 2001); A.B. 722 (N.Y. 2001); S.B. 218 (N.Y. 2001); S.B. 593 (N.Y. 2001); S.B. 373 (N.Y. 2001); H.B. 1045 (S.D. 2001); H.B. 241 (Tex. 2001); H.B. 358 (Tex. 2001); H.B. 1911 (Va. 2001); H.B. 2091 (Va. 2001); H.B. 1381 (Wash. 2001); S.B. 5364 (Wash. 2001); S.B. 12 (Wis. 2001); S.B. 15 (Wis. 2001).

112. Use and Misuse of Social Security Numbers, Hearings before the Subcomm. on Social Security of the House Comm. on Ways and Means, May 11, 2000 (statement of Stuart K. Pratt, Vice President, Government Relations, Associated Credit Bureaus, Inc.).

113. 429 U.S. 589 (1977).

114. Public Utilities Commission v. Pollack, 343 U.S. 451 (1952).

115. Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975).

116. Cohen v. California, 403 U.S. 15 (1971).

117. Martin v. Struthers, 319 U.S. 141 (1943).

118. Lamont v. Postmaster General, 381 U.S. 301 (1965).

119. Denver Area Educational Telecommunications Consortium, Inc. v. FCC, 518 U.S. 727 (1996).

120. New York Times Co. v. United States, 403 U.S. 713 (1971).

121. Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978).

122. Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

123. Florida Star v. B.J.F., 491 U.S. 524 (1989); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

124. Central Hudson Gas & Electric Corp. v. Public Service Comm'n, 447 U.S. 557, 566 (1980); Board of Trustees v. Fox, 492 U.S. 469, 480 (1989).

125. U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 528 U.S. 1188 (2000).

126. Id. at 1235 (quoting Rubin v. Coors Brewing Co., 514 U.S. 476, 486 (1995)).

127. U.S. West Communications, Inc. v. Federal Communications Comm'n, 528 U.S. 1188 (2000).

128. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).

129. Restatement (Second) of Torts § 652A (1976).

130. See, e.g., Florida Star v. B.J.F., 491 U.S. 524 (1989).

131. Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).

132. 12 C.F.R. §§ 40.3(o), 216.3(o), 332.3(o), 573.3(o).

133. 45 C.F.R. 160.103.

134. National Association of Attorneys General, supra at 10.

135. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (1999) (FTC, final rule) (codified at 16 C.F.R. pt. 312).